BEST AVAILABLE IMAGES

Defective images within this document are accurate representation of The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 1/00, 12/14

A1

(11) International Publication Number: WO 90/13865

(43) International Publication Date: 15 November 1990 (15.11.90)

(21) International Application Number: PCT/US90/02209

(22) International Filing Date: 24 April 1990 (24.04.90)

(30) Priority data:

345,083	28 April 1989 (28.04.89)	US
509,979	20 April 1990 (20.04.90)	US

(71) Applicant: SOFTEL, INC. [US/US]; 1200 Bayhill Drive, Suite 300, San Bruno, CA 94066 (US).

(72) Inventor: HORNBUCKLE, Gary, D. ; 1272 Padre Lane, Pebble Beach, CA 93953 (US).

(74) Agents: MURRAY, Leslie, G. et al.; Schroeder, Davis & Orliss Inc., P.O. Box 3080, Monterey, CA 93942 (US).

(81) Designated States: AT, AT (European patent), AU, BB, BE (European patent), BF (OAPI patent), BG, BJ (OAPI patent), BR, CA, CF (OAPI patent), CG (OAPI patent), + CH, CH (European patent), CM (OAPI patent), DE, + DE (European patent), DK, DK (European patent), ES (European patent), FI, FR (European patent), GA (OAPI patent), GB, GB (European patent), HU, IT (European patent), JP, KP, KR, LK, LU, LU (European patent), MC, MG, ML (OAPI patent), MR (OAPI patent), MW, NL, NL (European patent), NO, RO, SD, SE, SE (European patent), SN (OAPI patent), SU, TD (OAPI patent), TG (OAPI patent).

Published

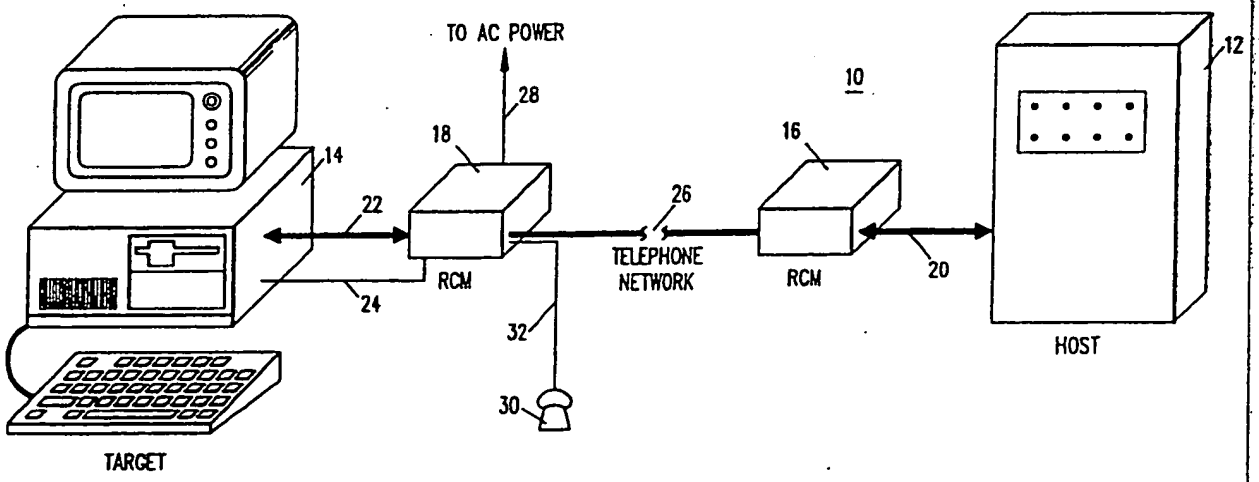
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

– decrypt software using user device-specific key

(PJ 19 +)

(54) Title: METHOD AND APPARATUS FOR REMOTELY CONTROLLING AND MONITORING THE USE OF COMPUTER SOFTWARE



(57) Abstract

Remote control of the use of computer data and video game software is described in a system for renting computer software which derives use and billing information, prevents unauthorized use, maintains integrity of the software and controls related intercomputer communications. A user at a target game or computer "downloads" programs or data, via a telephone line and remote control modules, from a central host computer. Usage of the video game and other program software or data by the target computer or other accounting data are recorded and stored and, at predetermined times, the host computer "uploads" the usage data for processing. Other features include: (1) software and usage security for rental software programs; (2) a polynomial generator/checker for generating block check characters for assuring integrity of data transmitted and received; (3) a voice-data switch for switching between data communication and normal telephone communication; and (4) and audio amplifier and speaker for monitoring of activity on the communication line during data transfers.

+ See back of page

DESIGNATIONS OF "DE"

Until further notice, any designation of "DE" in any international application whose international filing date is prior to October 3, 1990, shall have effect in the territory of the Federal Republic of Germany with the exception of the territory of the former German Democratic Republic.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MC	Monaco
AU	Australia	FI	Finland	MG	Madagascar
BB	Barbados	FR	France	ML	Mali
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Fasso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GR	Greece	NL	Netherlands
BJ	Benin	HU	Hungary	NO	Norway
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	SD	Sudan
CF	Central African Republic	KP	Democratic People's Republic of Korea	SE	Sweden
CG	Congo			SN	Senegal
CH	Switzerland	KR	Republic of Korea	SU	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
DE	Germany, Federal Republic of	LK	Sri Lanka	TG	Togo
DK	Denmark	LU	Luxembourg	US	United States of America

METHOD AND APPARATUS FOR REMOTELY CONTROLLING AND MONITORING THE USE OF COMPUTER SOFTWARE

Technical Field

The present invention relates to remotely controlling and monitoring the use of computer software. More particularly, this invention relates to a system for renting computer software products while 1) deriving customer use and billing information; 2) preventing unauthorized copying and use; 3) maintaining the integrity of the rented software product (hereafter also "package"); and 4) controlling related voice, program and data communications between the host and user's computers.

Background Art

For purposes of the present invention, rental computer software refers to the service of providing computer software to customers (hereafter also users) on a pay-as-used basis, where the software is executed on the customer's own personal computer. In the past, the only software offered for "rent" was software installed on centrally located computers, accessible via remotely located workstations or terminals. Such systems are well-known as "time-sharing" systems.

In time-share systems, software is executed on the central computer system, and not on the customer's own computer. Time-shared software is typically accessed over telephone networks using a "dumb" terminal or equivalent located at the customer's home or office. In such systems, all customers share the central computer resource, and the quality and delivery of services provided generally degrade, i.e., slow down, as more customers attempt to use the resource simultaneously. In addition to charges for the central computer to execute the users program (i.e. CPU time), charges for time-share usage must also include the cost for continuous use of the public telephone network for the duration of the connection to the central computer (i.e. connect time), whether or not the central computer is

actually executing the user's program. Thus, as the number of users increase, both CPU time and connect time increase; as CPU time and connect time increase, charges escalate as service degrades.

In general, and particularly in the circumstances just described, charges for use of software via time-share systems are likely to be much greater and far less predictable than for the rental of software which is executed on the customer's own computer. On the other hand, host-based, time-share systems have successfully provided software that is too expensive or complex to be made available on smaller systems such as personal computers. Thus it is desirable to continue offering expensive and complex software installed on host-based systems, while eliminating the disadvantages of time-share systems.

The software rental system of the present invention has some features which are not unlike pay-for-view television systems enjoyed by television viewers today. In pay-for-view television systems, the customer generally pays to watch a particular program. For that purpose, the customer is provided with a control box supplied by a cable television company. The control box, once activated from the cable company office, decrypts encrypted television signals transmitted to the user by the cable company. If the customer is not authorized to view a particular program, the image remains scrambled, and is unintelligible to the viewer. Conversely, once the customer has selected and paid for the program desired, the control box decrypts the signal and the program is understandable by the viewer.

In the relevant prior art, U.S. Patent No. 4,361,851 discloses a television usage monitoring system comprising a modified program selector (installed in the home of a subscriber) which is used to select television programs for viewing while, at the same time, providing the selection information to a remote monitoring unit (also installed in the subscriber's home). The remote monitoring unit is connected to the subscriber's telephone line and is programmed to periodically communicate, via

telephone lines, with a central computer for the purpose of transmitting the television usage data thereto. The disclosed remote monitoring system can be utilized for "[a]ccess to centralized public database networks" (see column 2, line 4). The system is also described as having the capability of producing a "disable" signal from the central computer to the remote unit if, for example, the subscriber has not timely paid charges due on his account. It should be noted that U.S. Patent No. 4,361,851 does not disclose a system for 1) secure and remotely controlled downloading and use of computer programs and data; 2) remotely controllable monitoring of use and security of the downloaded programs and data; and 3) accessing and retrieving stored usage data. In addition, neither means for generating block check characters for data transmitted and received, nor voice-data switching capability is described.

U.S. Patent No. 4,624,578 discloses a rental contract timer system for operating a relay to connect power to the rental equipment such as a television set, only during the time for which rental has been paid. A magnetic card reader determines, from an inserted card, the rental period and identifying information, and the timer contains a real-time clock and a microprocessor to compare the current time with the time in the rental period.

In addition, U.S. Patent No. 4,700,296 discloses an electronic access control system for controlling customer access to rental appliances located in the customer's home or other location away from the direct physical control of the renter. The system comprises a control module wired into the appliance with a card reader for programming the module to permit access and usage of the appliance by the customer.

Disclosure of Invention

In a software rental system according to the principles of the present invention, a control module is installed on or in cooperation with the customer's computer (hereafter also target computer), and the customer pays

for services, i.e., the use of the software, received. While operation of the system is as convenient to use, substantially different features, advantages and implementation with respect to the corresponding television system are necessary and desirable. Specifically, the customer in a software rental system may rent any program of an entire library of computer programs at any time, rather than waiting for a particular time slot during which a particular program would be available. Moreover, it is not necessary to install a separate transmission system, such as a TV cable system, to access programs, since they are downloaded over conventional telephone lines. Finally, the software available for rent is not broadcast over the entire system, but rather individual programs are down-loaded to the user's system from the host only after selection by the user.

The control module used in the proposed software rental system performs many more functions than its counterpart in the pay-for-view television system. For example, it controls and verifies that use of a program is authorized; it records the actual time that the program is used; and it protects the rental program from theft, copying, vandalism or modification. In addition, facilities for communication via the telephone lines between the control module installed at the user's site and the central or host computer are provided.

A software rental system according to the present invention is also efficient and highly automated, for performing a number of overhead functions. At the same time, in order to maximize customer satisfaction, the overhead activities of the control module are essentially transparent to the user. Thus, for example, accounting and billing activities are automated to avoid the need for manual "meter readers", and other control operations conventionally involving a high degree of overhead expense are reduced or eliminated where possible.

By means of the present invention, an authorized user at the target computer is able to "download" programs or data, via a telephone line and a programmable remote control module (RCM) connected at each end

thereof from a central or host computer. Usage and other accounting data are monitored by the RCM and stored in memory resident therein. At predetermined times, the central or host computer accesses the RCM for the purpose of "uploading" the usage and other accounting data to the central or host computer.

The RCM of the present invention also includes: (1) programmable modules for preventing unauthorized use, copying, vandalism and modification of downloadable data and programs during or after transmission to the target computer; (2) a polynomial generator/checker for generating block check characters for assuring the integrity of data and programs transmitted and received; (3) a voice-data switch for switching between data communication (with the central or host computer) and voice usage of the telephone line via the RCM; and (4) an audio amplifier and speaker so as to permit monitoring of activity on the communication line during data transfers by the RCM.

With the features listed above, the proposed system provides for error-free transmission of programs or other data between a host computer and a target computer, and for the secure transmission, reception and usage of programs or other data transferred between the host computer and the target computer. The audio amplifier and speaker can be used by the customer to monitor activity on the communication line during data transfers between the target and host computers. Finally, the RCM can be controlled to function as a conventional modem when conventional telecommunications service is desired. A voice/data selector switch is provided so that the user can select between voice and data communications.

The proposed software rental system has the capability to provide users with access to a wide range of software, including virtually all software that is sold for use on a personal computer. Thus, the system is particularly suited to the dissemination, on a pay-for-use basis, of otherwise expensive and complex software, such as certain engineering or scientific software, as well as certain financial accounting or tax programs.

The software rental system according to the present invention is further adaptable to the rental of video game software for use with well-known video game systems in combination with a home television set, for example, the well-known NINTENDO home video game computer systems. Desired video game software can be downloaded from a central or host computer by an authorized user via public telephone lines to the RCM which stores the game software for repeated use and monitors game usage. Since the game software is stored in the RCM memory, a telephone line connection is not required except to download additional game software and to transmit usage and other billing data to the host computer. A plug-in cartridge adapted to plug into a standard game cartridge slot provides the interface between the RCM and the video game system computer. A user makes a game selection via a joy stick or other input device provided with the video game system. For example, the host computer may transmit (i.e., download) a menu to be displayed on the user's television set screen providing a selection of games available for use. Additionally, the host computer may be utilized to transmit advertising and promotional material relating to new games and other services to be displayed with the game menu. Downloaded game software includes an encoded package identification number (PID) which is unique for each separate game software package. The PID is utilized for security of the software and to prevent unauthorized use of the game. Each use of the downloaded game software is internally recorded by the RCM and billed automatically by the host computer.

The system is also well-suited for allowing a customer to use moderately priced software on a rental basis to see if it really meets his needs. If satisfied, the software could be purchased, and marketing programs whereby the customer may apply some or all of the rental fees to the purchase price of the software could be devised. The proposed software rental system, therefore, offers software on a rental basis to new or low-usage customers at lower cost than would be otherwise incurred by purchase of the same software.

Rental software, as contemplated by the present invention, is less expensive than time-share software, and more convenient to use because execution is controlled by the user and unaffected by the number of other users. By eliminating the high initial cost of purchasing software and unpredictable cost and inconvenience of time-sharing, the number of users of a software rental system could be expected to grow indefinitely. Moreover, with more users becoming acquainted with various software products, the software industry as a whole would benefit, since the number of ultimate purchasers of the software would be likely to increase. Thus, with respect to both rental and purchase of software, the revenue of software vendors may be expected to increase.

The above and other objects, features and advantages, as will hereinafter appear, and the nature of the invention will be more fully understood by means of the detailed description set forth below, with reference to the associated drawings and the appended claims.

Brief Description of the Drawings

Figure 1 is an illustration of the data communication system in which a remote control module of the present invention is employed.

Figure 2 is a block diagram of the remote control module employed in accordance with the present invention.

Figures 3A and 3B are circuit diagrams of the remote control module shown in Figure 2.

Figure 4 is a system diagram illustrating the use of the remote control module of the present invention with a video game system.

Figure 5 is a block diagram of the remote control module shown in the video game system illustrated in Figure 4.

Best Mode for Carrying Out the Invention

Referring now to Figure 1, software rental system 10 generally comprises host computer 12, target computer 14, remote control module

(RCM) 16 associated with the host computer 12, and RCM 18 associated with the target computer 14. Communication between the host computer 12 and the target computer 14 and their respective RCMs 16 and 18 is accomplished via a standard serial RS232 communications link.

In operation, programs to be provided to authorized users on a rental basis are stored in the host computer 12. Typically, the host computer 12 is owned by a software rental service or company and is located at their offices. As shown in Figure 1, the host computer 12 is connected to the public switched telephone network 26 via serial data line 20 RCM 16.

The target computer 14 is the computer of any user, and may be a workstation, minicomputer, or even a mainframe. However, for purposes of software rental, the most likely target computer is expected to be a personal computer, owned and operated by a user in a home or office setting.

The target computer 14 is connected to telephone network 26 via serial data line 22 and RCM 18. RCM 18 is also connected to a conventional source of AC power via power line 28, which also can be provided to the target computer 14 by RCM 18 via power line 24.

In operation, the host computer 12 can "dial up" the target computer 14 and, conversely, the target computer 14 can "dial up" the host computer 12. Functions of the host computer 12 include transmission of software to the target computer 14, request for and reception of customer usage data associated with the target computer 14 from RCM 18, and performance of various accounting and software rental business functions.

RCMs 16 and 18 and the methods for using them which are disclosed herein are intended to work with any type of host computer 12 and target computer 14. The software installed in the host computer 12 and the target computer 14 will, of course, be different for different types of computers, but the methods remain the same.

In accordance with the present invention, at any given time, the

host computer 12 can communicate simultaneously with any number of target computers depending on the number of RCM's attached to, and the communications capacity of the host computer 12. Thus, by adding host computer RCMs and, if necessary, host computers, a virtually unlimited number of target computers 14 associated with RCMs 18 can simultaneously access rental software packages from the host computer(s).

Communication with the host computer 12 is an integral part of the software rental concept of the present invention, but the timing of communication of usage data to the host is not critical, since it is primarily for accounting and other administrative functions. Of course, the target computer(s) 14 can run rental software whenever and as often as the user desires.

Host computer 12 employs RCM 16 rather than merely a conventional modem to provide also for data integrity and program security. RCM 16 includes error detection circuits and data encryption modules for use in conjunction with communication from host computer 12.

Finally, as seen in Figure 1, telephone 30 may be connected to RCM 18 via telephone line 32, using standard RJ11 modular plugs. In addition, a switch (not shown) may be provided on the front panel (not shown) of RCM 18 for use by the customer to select voice or data modes of communication. In the voice mode, telephone 30 can be used to conduct voice communication over telephone network 26.

In a user's system wherein the target computer 14 comprises a number of target computers on a local area network system, only one RCM 18 associated with the local area network system is required. The target RCM 18 is coupled via the public telephone network through the user telephone PBX system to the host computer RCM 16 or, alternatively, the user may install a separate telephone line dedicated solely to the target RCM 18. Each of the target computers on the local area network may then communicate with the target RCM 18 via the local area network. Optionally, a multiplexing apparatus (not shown) may be incorporated in the RCM 18

output circuitry thus allowing simultaneous use by several target computers on the local area network.

Referring now also to Figures 2, 3A and 3B, RCM 16 comprises microprocessor 50, program memory 52, read/write memory 54, real-time clock (RTC) 56, power supply 58, priority interrupt control circuit 60, light-emitting diode (LED) displays 62, modem 64, dial access arrangement (DAA) 66, RS232 serial data interface 68, data encryption/decryption module 70, and polynomial generator and checker (PGC) 72.

Microprocessor 50 is any conventional microprocessor, but may be a multi-port integrated circuit device, such as an 8031 microprocessor, the ROM-less version of the 8051 microprocessor 50 (Figure 2) and the speed of the communications link between the host computer 12 and the target computer 14 (Figure 1) are not critical to systems constructed according to the principles of the present invention. Thus, while higher speed communication is typically superior to lower speed communication, the only requirement is that microprocessor 50 be fast enough to implement the various tasks that it is called upon to perform in its operating environment.

Program memory 52 is any conventional read-only memory (ROM) and is used to store the program executed by microprocessor 50 in performing the functions of RCM 18. An erasable/programmable read-only memory (EPROM), e.g., a 27128, may be used for program memory 52 when the modification of functions performed by RCM 18 may be desirable. However, an equivalent conventional ROM is acceptable and, typically, is a lower cost device.

Read/write memory 54 is, preferably, implemented by a Toshiba TC5565 static random access memory (RAM) having a capacity of at least 8 kilobytes. Back-up battery power is provided by power supply 58 to ensure that the contents of memory 54 are not lost if power to the RCM 18 is interrupted.

RTC 56 is, preferably, an ICM 7170 device manufactured by Intersil. The latter circuit maintains the date and time to the nearest 0.01

second. The occurrence of a leap year is automatically accommodated. RTC 56 is connected to the power supply 58 and receives battery backup therefrom in case of power failure. RTC 56 functions in a conventional manner to provide control and time information, upon request, to microprocessor 50. This enables the RCM 18 to perform its function of developing time, accounting and billing data relative to customer access to and use of programs initially stored in the host computer 12. Such time and billing data are provided to the host computer 12 by RCM 18 on command from the host computer 12.

Power supply 58 provides direct current power to the various other circuit elements of the RCM 18. In the event of a power failure or turning off of the AC power to the RCM 18, a "battery backup" feature of the present invention detects such condition, and the internal battery of RCM 18 provides battery backup power to the read/write memory 54 to protect data stored therein, and to RTC 56 to maintain operation thereof. In this manner, the contents of the memory 54 and the operation of the RTC 56 are not disturbed by a loss of AC power. Preferably, the internal battery of power supply 58 is a conventional rechargeable battery such as to preserve the contents of memory 54 and maintain operation of RTC 56 for several years, if necessary. Once AC power is restored to the system, the internal battery returns to its "wait" state, and power is not expended by the internal battery.

RCM 18 is provided with one standard 110 VAC output receptacle for receiving the standard electrical power plug for the target computer 14. The receptacle is relay-controlled so that switched AC power output is provided to the target computer 14 via power line 24. In this manner, target computer 14 can be turned on or off by RCM 18 for certain functions as described elsewhere in this specification.

Device interrupts generated within RCM 18 of Figure 2 are merged in priority interrupt control circuit 60, which comprises a 74LS348 integrated circuit chip. Microprocessor 50 supports only two priority

interrupts, namely, INT0 and INT1. INT0 is unassigned and is available as a test point for use with various test equipment. All other interrupts are assigned to INT1. Since all of the devices of RCM 18 have separate interrupt enabling control, any or none of the device interrupts may be used.

The nature and source of a particular interrupt is determined by reading terminals P10-P12 (as shown in Figure 3A) of interrupt control circuit 60. Once an interrupt has occurred, its cause must be resolved by microprocessor 50, or the same interrupt will continue to recur. A summary of typical interrupts and their priorities is given in Table 1 below.

Interrupt	Value of P10-P12	Priority
Power low	0	Highest
Incoming ring	1	Next Highest
Modem Interrupt	2	Next Highest
UART	3	Next Highest
RTC	4	Next Highest
PGC	5	Lowest

LED displays 62 comprise a number of single light emitting diode displays to indicate the status of certain conditions and the occurrence of certain events. Such conditions or events include power-on, power-off, and the status of communications activity. During diagnostic and test functions, the LED displays take on different meanings related to these functions.

Modem 64 includes modulation and demodulation circuitry for sending and receiving data over the public switched telephone network 26 (Figure 1). Preferably, modem 64 is implemented by a 73K222 modem circuit (for 300, 600 and 1200 baud) or a 73K224 modem circuit (for 2400 baud) manufactured by Silicon Systems, Inc. However, other conventional modem circuits, including modem circuits supporting higher baud rates, can be used to implement the functions of modem 64. Moreover, since modem 64 can

serve as a standard personal computer type modem when the target computer 14 is not engaged in accessing rental software, it is not necessary to include an additional modem for communication with other computer services or data base services.

Dial access arrangement (DAA) 66 provides for connection of RCM 18 to the public switched telephone network 26. DAA 66 connects private circuits to the public switched telephone network in compliance with FCC regulations, Part 68. Thus, DAA 66 includes transformer isolation, impedance matching circuits, ring detection circuits, voice/data switching circuits, hook relays and other well-known circuitry required for connecting to the public switched telephone network 26.

The serial data interface 68 is a conventional serial interface for communication in accordance with standard RS232 criteria. More specifically, interface 68 is, preferably, a universal asynchronous receiver/transmitter (UART), model SCC2691, for carrying on serial data communication between RCM 18 and the target computer 14. Thus, the interface 68 is coupled to a standard RS232 serial port of the target computer 14 via serial data cable 22. Data is transmitted serially between the target computer 14 and interface 68, whereas data is transmitted in parallel on bus 74 between interface 68 and microprocessor 50.

Further considering the serial link between interface 68 and the target computer 14, the clock for the serial port of the target computer 14 has a frequency equal to one-fourth the frequency of the internal clock of microprocessor 50 of RCM 18. Preferably, the frequency of the serial port clock of the target computer 14 is set to 2.7648 MHz.

The baud rate between the RCM 18 and the target computer 14 may be any value, provided that the RCM 18 can buffer the data. The baud rate of the modem 64 is set to 300, 600 or 1200 baud, depending on the transmission method chosen.

Data encryption/decryption module 70 performs a decrypting function with respect to data received by RCM 18, from the host computer

12. Data decrypted by module 70 of RCM 18 was encrypted by a corresponding data encryption/decryption module in RCM 16 associated with the host computer 12 prior to transmission to the RCM 18. The encryption and decryption functions will be discussed in more detail herein below in connection with a more complete discussion of the software security technique employed by the present invention.

Polynomial generator/checker (PGC) 72 is, preferably, an SCN2653 device manufactured by Signetics, Inc. Preferably, RCM 18 generates block check characters (BCC) for each block of data to be transmitted by RCM 18 to the host computer 12. Correspondingly, each block of data received from the host computer 12 by RCM 18 is checked in accordance with the BCC. By way of a further preference, PGC 72 employs a CRC-16 polynomial code with an $X^{16} + X^{15} + X^2 + 1$ divisor. In this manner, all single-bit errors and most multiple-bit errors are detected. The CRC-16 polynomial is employed because the error codes generated are much more reliable than the normal "check sums" typically used. This is especially true for data transmitted over the public switched telephone network 26.

Since data communications using the public switched or dial-up telephone network 26 are notoriously error prone, special precautions are often taken to at least detect errors, if not correct them. More elaborate schemes can be used to correct the errors, and such error-correction coding schemes are not precluded by the present design of the RCM 18. However, for reasons of economy and speed in data communications, the preferred embodiment described herein performs error detection only. In the present system, a data block is simply retransmitted in the event of an error detection.

As generally discussed above, the error detection method employed herein involves the transmission of a specially generated 16-bit code at the end of each data block. The check code is generated by PGC 72 using the aforementioned CRC-16 polynomial with the aforementioned divisor. At the receiving end, the check code is, in effect, regenerated and

compared to the actual check code received. If identity is not present, a transmission error has occurred and an error signal is generated by PGC 72. Once an error is detected, a request for retransmission is initiated and the data block will be retransmitted by the host computer 12 to RCM 18, or from RCM 18 to the host computer 12, as the case may be.

The check code employed herein can be mathematically shown to be very effective in detecting the types of errors that normally occur over public switched or dial up telephone networks such as network 26 (Figure 1). Simpler schemes could be implemented, and would not require the use of PGC 72, but such schemes are not as effective for this application.

Accordingly, all communication between the host computer 12 and target computer 14 or RCM 18 employ the above-described error detection method with retransmission of data blocks upon detection of errors. In the latter regard, RCM 18 employs PGC 72 for checking data received from host computer 12, and a corresponding PGC in RCM 16 (Figure 1) checks data received from the target computer 14 or RCM 18.

Certain applications of the system 10 (as shown in Figure 1), in particular for the business of software rental, typically will be configured so that the host computer 12 sends and receives data/messages to and from the target computer 14 over the public switched telephone network 26. As also indicated above, RCMs 16 and 18 serve as interface devices to connect the host computer 12 and the target computer 14, respectively, to the telephone network 26. Obviously, while designed to work with the public switched telephone network the present invention can be configured to work with any communications link between the host and target computers.

The circuit configurations of RCMs 16 and 18 are identical. The operation of the RCM 18 associated with target computer 14 and the operation of RCM 16 associated with host computer 12 is determined by program instructions executed by microprocessor 50.

RCMs 16 and 18 provide serial communication, via RS232 serial data interface 68, to the host computer 12 and target computer 14,

respectively, each of which is preferably located within a short-distance (i.e., a few feet) of its respective RCM. Whereas a single RCM 18 is required for each target computer 14, a plurality of RCMs 16 may be used with host computer 12. In fact, the number of RCMs 16 must be equal to the number of simultaneous data-transmission links between the host computer 12 and target computers 14 (to download software) or RCMs 18 (to upload usage and accounting data). In this manner, the host computer 12 can carry on data conversations with several target computers 14 simultaneously.

When a customer contracts to participate in the rental software system, the software rental company will provide the customer, either through sale or rental, with RCM 18 for connection to and association with the customer's target computer 14. Installation of the RCM 18 is easily performed by the customer. Referring again to Figure 1, RCM 18 is connected to the public telephone network 26 by means of a standard RJ11 type modular telephone cord extending between RCM 18 and the telephone system jack. In addition, RCM 18 is connected to the target computer 14 via a serial data cable 22 and power cable 24, RCM 18 deriving its power from a conventional AC power source via cable 28. As an option, telephone (or telephone handset) 30 may also be connected to RCM 18 via telephone cable 32 utilizing standard RJ11 modular plugs. Thus, when RCM 18 is not being used for data communications, the telephone 30 can be used for normal voice communications. When data communications involving RCM 18 are to take place, RCM 18 performs automatic switching so as to break the connection between telephone 30 and telephone network 26, and to establish connection between DAA 66 (Figure 2) and the network 26.

During preprogrammed times, as established by the software of the host computer 12 and transmitted to RCM 18 and stored in memory 52 of RCM 18, RCM 18 will initiate an "automatic answer" mode of operation so that it may respond to messages received from the host computer 12. Such communications between the host computer 12 and the target computer 14 normally occur at night so as to take advantage of low telephone rates

in effect at that time, and also to avoid conflicts with other data transmission functions of target computer 14.

The RCM 18 can also be used as a standard modem for the target computer 14, and can be set up to communicate with remote computer or other database services. RCM 18 distinguishes between its usage as a standard modem and its usage as a special remote control module for controlling access to rental software.

During the time that RCM 18 is not performing data communications and is not set up in its "automatic answer" mode, telephone 30 (if one is attached) is available for normal use,, and will ring in the usual way when called.

One feature of the proposed software rental system is the ability to download software from the host computer 12 to target computer 14 during off-peak hours, such as late at night. Preferably, the customer will not be compelled to participate in or supervise the downloading of software during such late-night hours. Thus RCM 18 is able to control the AC power provided to the target computer 14 in response to control signals from the host computer 12. In order to enable this feature of the present invention, the on/off switch of target computer 14 is left in the "on" position, and the power cable 24 (Figure 1) of target computer 14 is plugged into a receptacle 102 at the rear of RCM 18, RCM 18 being connected via its own power cord 28 to an AC power source, as previously described. Preferably, the front control panel of RCM 18 is provided with an on/off switch so that the customer can turn on or turn off the target computer 14 manually. However, this switch is preempted when RCM 18 receives a command from the host computer 12 to turn on the target computer 14 for late-night operation.

Accordingly, when downloading of software is desired, the host computer 12 calls the target computer 14, and once the call is acknowledged by RCM 18, the host computer 12 turns on the target computer 14 by actuating the AC power switch in power supply 58 (Figure 2). When the

target computer 14 is turned on by RCM 18 at the command of the host computer 12, the host computer 12 can download software to a storage device (not shown) associated with the target computer 14. In addition, for reasons described below, a special patch for the target computer 14 operating system, which is required to run the rental software, is also downloaded (if not previously downloaded) from the host computer 12 to the target computer 14. Once the software downloading process is complete, the host computer 12 commands RCM 18 to turn off power to the target computer 14.

Power to non-essential external peripheral devices associated with target computer 14, such as a printer, a display device and the like, need not be controlled through RCM 18 since the downloading process does not require the use of such external peripherals. However, if desired, such external peripheral devices may be controlled through the RCM 18 by making appropriate power connections to the RCM 18.

Referring again to Figure 2, RCM 18 contains a program memory 52 and a read/write memory 54. The program memory 52 holds the program instructions which microprocessor 50 implements in order to accomplish the functions of RCM 18. Read/write memory 54 holds the accounting data relating to software rental by the user of the target computer 14, and also provides buffer storage for communications messages passing between the host computer 12 and the target computer 14. Read/write memory 54 may also store other ancillary data.

RTC 56 is included in RCM 18 in order to provide a real-time time-base, including exact year, month, day and time. Preferably, accuracy is to the nearest 0.01 second. The setting of RTC 56 with the year, month, day and time is strictly controlled by the host computer 12 using security techniques available to it through data encryption/decryption module 70.

Overall, RCM 18 is a real-time controller that can be called into action independently by host computer 12, target computer 14, a change of state of the power switches of RCM 18, and other internal conditions. Accordingly, an interrupt system is designed into the operation of RCM 18,

and is used to enable microprocessor 50 to manage these independently occurring real-time events. The management of interrupts by microprocessor 50 is assisted by priority interrupt control circuits 60.

An important aspect of the present invention concerns security for rental software executed by the target computer 14 (Figure 1). This software security function is provided by the cooperation of data encryption/decryption module 70 in RCM 18 with a corresponding data encryption/decryption module in RCM 16 associated with the host computer 12. Closely coupled with the function of providing software security is the function of keeping track of and accounting for the time periods during which the target computer 14 is using the rental software on which the rental charges are based.

In at least some instances, the rental software provided by the host computer 12 may have a very large amount of code and many data files. Of course, it is not necessary to provide security or protection for each and every component or module of most rental programs. In accordance with the present invention, a particularly critical module --hereinafter referred to as the "key module" -- in each rental program is identified. The key module, according to the present invention is essential to program execution and without which the overall rental program will not run.

In addition to identification of the key module, the security of rental software according to the present invention also requires a special version of the operating system to be utilized in the target computer 14. The special version of the target computer operating system is created by a patch module, hereinafter "operating system patch module" or "OSP" module (the OSP is identical for all rental software executed on target computers of the same or similar type), which is downloaded to the target computer 14 along with the rental software. The OSP module initiates decryption of the encrypted key module of the rental software package by module 70 of RCM 18, then loads the decrypted key module into the internal memory (not shown) of the target computer 14 for execution. In addition, periodically

while the rental software package is running, the OSP module communicates with the RCM 18 to provide verification that it is still connected to the target computer 14 for security and accounting purposes.

The key module is encrypted using the Federal Information Processing Data Encryption Standard No. 46, well-known to those of skill in the art, by the data encryption/decryption module 70 of RCM 16. When the rental software is transmitted by the host computer 12 over the telephone network 26, the encrypted key module and the associated OSP module are transmitted as well. Alternatively, the encrypted module, the OSP module and the unencrypted remainder of the rental software may be sent to the customer on floppy disks, optical disks, a compact disk ROM, for example, or magnetic tape by mail or other delivery service. If utilizing a magnetic or optical disk device, the target RCM 18 would also incorporate a well-known SCSI drive interface thus allowing the encrypted software and data to be accessed via the RCM 18. When downloaded from the host computer 12 or loaded from media otherwise provided by a software rental service, the entire rental software package (including the encrypted key module and OSP module) is stored in a peripheral storage device (e.g., hard disk or floppy disk) associated with the target computer 14.

Further referring to the encryption process of the present invention, data encryption/decryption module 70 of RCM 16 uses an encryption key unique to the individual target computer in which the rental software is to be used. Methods of encrypting and decrypting using an encryption key, such as described in U.S. Patent No. 4,649,233, are well-known. However, since the encryption key is an important element which the software security scheme of the present invention depends, the encryption key itself is always transmitted in encrypted form to RCM 18 (utilizing an encryption key identical to the encryption key provided in RCM 18) to assure proper systems operation and integrity. When transmitted from RCM 16, the encryption key is then automatically decrypted as it is received by RCM 18 using a second, special key built into RCM 18 which is unique

to each individual RCM 18. The decrypted encryption key is then stored in the RCM memory 52 until decryption of a key module is required. Since the encryption key is retained in memory 52, the encryption key need only be transmitted to RCM 18 one time. If the RCM 18 is tampered with in any manner, the encryption key is destroyed. Without the encryption key, decryption of the key module of the rental software at the target computer 14 is essentially impossible, and use, copying, vandalizing or modification of the rental software is prevented. The security technique employed by the present invention also provides a high degree of protection during downloading of the package via the public telephone network 26 owing to encryption of the key module and of the encryption key.

As described above, decryption of the key module is performed in the data encryption/decryption module 70 of RCM 18. The encryption key used in the decryption process is inaccessible to the user. Thus, in accordance with the present invention, a downloaded rental software package will only run on the particular target computer 14 having an encryption key corresponding to the encryption key employed by the host computer 12 when the key module of the rental software package was encrypted. Since the rental software will operate only on a target computer 14 serviced by an RCM 18 utilizing an encryption key unique to the target computer 14 (to decrypt the key module), no other physical or licensing restrictions on the user's ability to make copies of the rental software package are required.

Prior to a customer executing a rental software package on a target computer, the software package will have been transmitted electronically or by other suitable means and be resident in a peripheral storage device associated with the customer's target computer. The rental software package will have the corresponding OSP module appended and the original key module will be replaced with an identical encrypted key module.

Assuming that a customer wishes to run a rental software

package protected in accordance with the present invention, the user follows exactly the same procedures for loading the software package from the associated peripheral storage device to the internal memory of target computer 14 as if an unrented version of the same package were being run. However, in a manner transparent to the user, when the key module of the software package is retrieved from the peripheral storage device of target computer 14, the OSP software module is activated. The OSP module fetches the encrypted version of the key module from the peripheral storage device (not shown) and sends it to the RCM 18 for decryption by the encryption/decryption module 70. After decryption, the key module is sent back to the target computer 14 and loaded into its internal memory (RAM) for execution. At the latter step the OSP module also initiates a timer controlled by the RTC 56 to begin recording the actual use time of the rental program for computation of rental time charges.

The rental program with the decrypted key module now stored in the internal memory of target computer 14 will operate in exactly the same manner as it would if it were not a rental package (i.e., the same way as if it were a purchased program). However, when execution of the rental program is complete, control reverts back to the OSP module. The OSP module then automatically erases the rental program including the key module from the RAM of target computer 14 and notifies RCM 18 that the period of use or rental period has stopped. The elapsed time between the starting and stopping of the rental program, as well as the time and date information, are recorded in memory 54 of RCM 18 for subsequent, off-line processing.

It is essential that the RCM 18 be connected to the target computer 14 at the time that the rental period ends. Connection of RCM 18 to the target computer 14 insures that the exact time of termination of the rental period is recorded. Furthermore, to maintain proper security of the rental software in accordance with the present invention, while the rental software package is running, periodically control is passed to the OSP

module upon the occurrence of certain periodic events, disk access by the target computer 14 operating system for example. The OSP module then executes routines to prevent circumvention of the rental accounting for use of the rental software package, and to protect the rental software package from theft, vandalism or other unauthorized modification. In particular, the OSP module then queries RCM 18 and verifies, through its response, that RCM 18 is, in fact, connected to the target computer 14. If it is, execution of the rented software continues; if it is not, the execution is terminated by the OSP module and the entire rental software program is erased from the target computer 14 RAM.

It should be noted that the rental software package itself may be modified by adding code to ascertain that the RCM 18 is connected to the target computer 14 rather than modifying the operating system by adding the OSP module for receiving control from the rental software package. However, since modifying the rental package is difficult without assistance from the developers of the package, adding the OSP module is preferable. Therefore, an operating system, so patched, must be used when executing rental software according to the present invention. As described above, the OSP module is downloaded with the rental software package, if it has not already been downloaded earlier with another software package.

The software security scheme of the present invention involves encryption of only the key module of the rental software in a predetermined algorithmic manner using an encryption key. Further, the encryption key itself is encrypted and transmitted by the host computer 12 separately. No changes to the functions of the rental software are made during the encryption process. Thus, any software package may be rented without technical involvement of the software vendor, and all of the security procedures are transparent to the user.

In accordance with the present invention, microprocessor 50 in RCM 18 is programmed to destroy an encryption key if: (1) the RCM 18 is physically tampered with; (2) the telephone number of the target

computer 14 is changed without notice or the telephone is disconnected for longer than a preselected period of time (in this case, destruction of the protection key takes place only after power is restored). If the encryption key is destroyed by the RCM 18, RCM 18 will attempt to notify the user by using a special alarm, such as a beeping sound or LED display. The host computer 12 also will be automatically notified by RCM 18, if possible. Restoration of the encryption key is then possible at the option of the rental software company.

Referring now also to Figure 4, another preferred embodiment of the present invention providing a video game software rental system is illustrated. Video game system 11 comprises central or host computer 12, remote control module (RCM) 29 associated with host computer 12, target game computer 15, television or monitor 13, RCM 21 associated with the game computer 15, interface cartridge 27 coupling the RCM 21 to the game computer 15 and game control input device 19. Similarly, as described hereinabove with regard to Figure 1, communication between the host computer 12 and the game computer 15 and their respective RCMs 29 and 21 is accomplished via a standard serial RS232 communication link or other suitable communication link. In operation, the host computer 12 is linked to the game computer's RCM 21 via the host RCM 29 and the public switched telephone network 26. Typically, available game software is stored in the host computer 12 which is centrally located in order to provide rental service to a large number of authorized users.

The target game computer 15 may be any of several well-known video game computer systems, such as that manufactured by Nintendo Company, typically owned and utilized by a user in a home or recreational setting in combination with a television or monitor. The game computer 15 conventionally utilizes readily available plug-in ROM game cartridges (not shown) which a user purchases. The game computer 15 and hence the progress of the game being played is controlled by well-known control devices 19 such as a joy stick or a combination of rocker switches and

buttons. The output of the game computer is coupled to the television 13 via cable 31 and typically comprises video and audio signals generated by the game computer 15 under the control of the game software and the user via user input device 19. AC power adapter 25 provides power to the game computer 15.

Referring now also to Figure 5, RCM 21 comprises microprocessor 51, program memory 53 (RAM) read/write memory 55 (also RAM), real-time clock (RTC) 57, power supply 59, priority interrupt control circuit 61, light-emitting diode (LED) displays 63, modem 65, dial access module (DAA) 67, input/output (I/O) connector 69, data encryption/decryption module 71 and data compression and error correction module 73. Both RCMs 21 and 29 operate similarly to RCMs 16 and 18 as described hereinabove with reference to Figures 2, 3A and 3B and only the differences in operation and detail therebetween will be further described herein. RCM 21 is coupled to the game computer 15 via I/O connector 69, data cable 33 and data interface module 75. The data interface module 75 is incorporated in a plug-in cartridge 27 adapted for use with the cartridge slot provided in the game computer 15 console. The data interface module 75 may comprise an RS232 serial data interface or other suitable data interface as required by the particular game computer 15 utilized by a user. The data interface module utilized in RCM 29 associated with the host computer 12 comprises an RS232 serial data interface 68 as described hereinabove with regard to RCM 16 and Figure 2.

When a customer contracts to participate in the video game software rental system, the software rental company will provide the customer, either through sale or rental, with RCM 21 and plug-in interface cartridge 27 for connection to and association with the customer's game computer 15. The type plug-in interface cartridge 27 provided is determined by the particular game computer 15 utilized by the customer. Referring again to Figures 1 and 4, RCM 21 is connected to the public telephone network 26 by means of a standard RJ11 type modular telephone cord extending between RCM 21

and the telephone system jack (not shown). The RCM 21 is connected to the game computer 15 via a serial data cable 33 and switched power cable 24 integrated therewith. In addition, RCM 21 is connected to a conventional AC power source via power cable 28. A dedicated telephone line may be provided for RCM 21 or, alternatively, a common telephone line may be shared between telephone 30 and RCM 21. Thus, when RCM 21 is not being used for data communications, the telephone 30 can be used for normal voice communications. When data communications involving RCM 21 are to take place, RCM 21 performs automatic switching so as to break the connection between telephone 30 and telephone network 26 (as shown in Figure 2), and to establish connection between DAA 67 and the telephone network 26.

The RCM 21 comprises a real time communications controller that can be initiated independently either by the host computer 12 or by the customer or user via game computer 15. When a user desires to have a selected video game software downloaded, the user initiates RCM 21 via the game computer 15 thus establishing a communications between RCM 21 and the host computer 12. Game software downloaded to RCM 21 in accordance with the user's instructions is stored in the read/write memory 55 for immediate and future use by the customer. Transfer or uploading to the host computer 12 of billing and usage data stored in the read/write memory 55 is initiated by the host computer 12 as described hereinabove. Billing and usage data is uploaded to the host computer 12 each time game software is downloaded. Further, host computer 12 may initiate RCM 21 at preprogrammed times automatically for uploading of billing and usage data.

When a user desires to play a video game, the user turns on the game computer 15 and RCM 21 via switched power cable 24. A game menu providing a list and description of available game software packages is called up and displayed on the television 13 screen. The menu is stored in read/write memory 55 and is periodically updated by host computer 12. The user selects a desired video game from the menu via input device 19. If the

selected video game has already been downloaded from the host computer 12 and stored in read/write memory 55, the selected video game software is retrieved by the game computer 15 for use and usage data stored in read/write memory 55. If the selected game software is not already stored in read/write memory 55, the user initiates communications with the host computer via RCM 21. The desired video game software is then downloaded and stored in read/write memory 55 and the communications link with the host computer 12 terminated. The game computer 15 then retrieves the selected video game software for use. Since it is not required that the RCM 21 be linked to the host computer 12 except during the time that game software is actually being downloaded, charges for use of the telephone network are not incurred during the time the user is actually playing the selected video game.

Security of and prevention of unauthorized use for the rental game software downloaded by the host computer 12 is provided by the cooperation of the data encryption/decryption module 70 in RCM 29 and the data encryption/decryption module 71 in RCM 21. Closely associated with the function of providing rental software security is the function of keeping track of an accounting for the time periods during which the game computer 15 is utilizing the game software on which the original charges are based.

Each game software package for each different game available for rental is assigned an 8-character package identifier code which is unique to the particular game provided by the game software package. Each software package is encrypted with a package key, the package key being the unique package identifier associated with each different game available. The entire software package may be encrypted or only selected critical portions or modules of the software are encrypted as described hereinabove. When a user signs up for a particular package, the package key associated with the software package is downloaded to the RCM 21 associated with the user's game computer 15. To protect the package identifier from unauthorized access while in transmission, the package identifier is encrypted for

transmission utilizing a unique user identifier code to encrypt the package key. A unique user identifier code is assigned to each user contracting with the software rental system and is stored in RCM 21 associated with the user's game computer 15. Since all game software packages associated with a particular game are identically encrypted, a particular game software package is required to be encrypted and fully tested once only thus allowing duplicate software packages to be provided, such as on floppy disk, for inventory. Once an encrypted game software package has been downloaded from the host computer 12 or otherwise input to the RCM 21 and stored in read/write memory 55, it may be retrieved and used repeatably as long as the user is authorized.

Typically a video game will comprise at least 200,000 bytes of data. In order to store a useable number of different video games, read/write memory 55 must have sufficiently large capacity, necessitating large blocks of addressable RAM. Read/write memory 55 may be a solid state memory block or, alternatively, may be an external storage module such as a magnetic disk drive. Further, because of the relatively large software programs be used, the data transmission rate becomes critical to the success of a video game rental software system. Well-known data compression techniques may be employed to reduce the transmission time required for downloading the game software packages. For a data transmission of 9,600 baud, the transmission time for 200,000 bytes is at least 200 seconds, or 3.3 minutes. Utilizing presently known data compression techniques allows the transmission time for this example to be reduced to approximately 1 minute. As discussed hereinabove, error correction techniques are utilized to compensate for the relatively high data error rates encountered with the public telephone networks.

While preferred forms and arrangements have been described in illustrating the present invention, it is to be understood that various changes in detail and arrangement may be made without departing from the spirit of the present invention or from the scope of the appended claims.

Claims

I claim:

1. Apparatus for controlling the use by a second computer of information stored in a first computer, said apparatus comprising:

first transmitting and receiving means coupled to said first computer for transmitting information to said second computer; and

a second transmitting and receiving means coupled to said first transmitting and receiving means and to said second computer for receiving information transmitted by said first computer;

said first and second transmitting and receiving means each including encryption/decryption means for encrypting and decrypting, respectively, preselected portions of the information, said preselected portions including application program information, and a first encryption key for encrypting and decrypting said preselected portions of the information including, said application program information;

said first and second transmitting and receiving means each including a second encryption key for encrypting and decrypting, respectively, said first encryption key.

2. Apparatus as in Claim 1 further including monitoring means for monitoring usage by said second computer of the information transmitted to said second computer for developing time accounting data relative to rental charges for said usage, and for preventing usage of the information if said second transmitting and receiving means is disconnected from said second computer.

3. Apparatus as in Claim 2 further including memory means coupled to said monitoring means for storing said time accounting data, said second transmitting and receiving means being responsive to a second command from said first computer for transmitting said time accounting data to said first computer.

4. Apparatus as in Claim 3 further including:

error detection means for detecting the presence of an error in said time accounting data transmitted by said second transmitting and receiving means and for producing an error signal; and

retransmission means coupled to said error detection means and responsive to said error signal for producing a signal representing a request for retransmission of said time accounting data, said second transmitting and receiving means responsive to said request for retransmission for retransmitting said time accounting data.

5. Apparatus as in Claim 1 wherein:

said encryption/decryption means in said second transmitting and receiving means decrypts the encrypted portion of the application program information only upon request of a user of said second computer to use the information, said second transmitting and receiving means thereupon transmits the decrypted information to said second computer.

6. Apparatus as in Claim 1 further including:

error detection means for detecting the presence of an error in the information transmitted by said first transmitting and receiving means and for producing an error signal; and

retransmission means coupled to said error detection means and responsive to said error signal for producing a signal representing a request for retransmission of the information transmitted by said first computer, said first transmission and receiving means being responsive to said request for retransmission for retransmitting the information.

7. Apparatus as in Claim 1 wherein said first and second transmitting and receiving means are coupled to each other via a public communication network.

8. Apparatus as in Claim 7 wherein said first and second transmitting and receiving means each include connection means for connecting said first and second transmitting and receiving means, respectively, to said public communications means.

9. Apparatus as in Claim 8 further including a telephone

coupled to said connection means associated with said second transmitting and receiving means, said connection means including means for connecting said telephone to said public communications network when said second transmitting and receiving means is not receiving the information and said transmitting means is not transmitting said time accounting data.

10. A remote control device for controlling and monitoring the use of computer software and data programs in a computer, said remote control device comprising:

first coupling means coupling said remote control device to said computer for transferring preselected portions of said software and data programs between said remote control device and said computer;

monitoring means for monitoring usage of said software and data programs in said computer and for developing time accounting data relative to said usage; and

decryption means coupled to said first coupling means for decrypting preselected encrypted portions of said software and data programs, said decryption means including a first encryption key for decrypting said preselected encrypted portions of said software and data programs, said first coupling means responsive to a load program to transfer said preselected encrypted portions of said software and data programs from said computer to said decryption means when said software and data programs are loaded into said computer, said decryption means responsive to said load program to decrypt said preselected encrypted portions of said software and data programs, said first coupling means responsive to said load program to transfer said decrypted preselected portions of said software and data programs from said decryption means to said computer for execution, said monitoring means responsive to said load program upon the transfer of said decrypted preselected portions of said software and data programs from said decryption means to said computer to initiate monitoring of said usage.

11. A remote control device as in Claim 10 further comprising:

second coupling means coupling said remote control device to a host computer via a communications link; and

transmitting and receiving means coupled between said first and second coupling means and to said monitoring means for receiving preselected computer software and data programs transmitted from said host computer for further transfer to said computer, said transmitting and receiving means responsive to a first command transmitted by said host computer to transmit said time accounting data concerning said usage from said monitoring means to said host computer.

12. A remote control device as in Claim 11 wherein said transmitting and receiving means comprises a modem and said communications link comprises a public telephone network.

13. A remote control device as in Claim 11 further comprising error detection means for detecting the presence of an error in blocks of said preselected computer software and data programs transmitted from said host computer and for generating an error signal when an error is so detected.

14. A remote control device as in Claim 13 wherein said error detection means includes error correction means for generating error-correction codes to correct any errors so detected in said preselected computer software and data programs.

15. A remote control device as in Claim 13 wherein said error detection means includes retransmission means responsive to said error signal to generate a retransmission request signal, said host computer responsive to said retransmission request signal for retransmitting said blocks of computer software and data programs containing errors.

16. A remote control device as in Claim 11 wherein said monitoring means includes timing means for providing timing information and generating a clock signal for use in said remote control device.

17. A remote control device as in Claim 16 wherein said monitoring means further includes memory means for storing said time accounting data, said transmitting and receiving means responsive at

preprogrammed times to said first command to transmit said time accounting data to said host computer.

18. A remote control device as in Claim 11 wherein said encryption and decryption means further includes a second encryption key for decrypting said first encryption key, said first encryption key transmitted from said host computer in an encrypted format.

19. A remote control device as in Claim 10 wherein said decryption means includes a second encryption key for decrypting said first encryption key.

20. A method of protecting the security of a computer software and data program comprising the steps of:

selecting a key module of said software and data program essential to the operation of the program, said software and data program not operable without said key module;

encrypting said key module with a first encryption key; and

decrypting said encrypted key module utilizing said first encryption key in a decryption means associated with a computer on which said software and data program is to be run, said first encryption key unique to said computer, said decryption means coupled to said computer.

21. The method of Claim 20 including the further steps of:

modifying the operating system of said computer in which said software and data program is to be run utilizing an operating system modification routine, said operating system modification routine initiating the decryption of said key module;

adding said operating system modification routine to said software and data program.

22. The method of Claim 21 including the further step of monitoring with monitoring means the usage by said computer of said software and data programs, said operating system modification routine initiating a clock to measure the period of said usage for developing time accounting data, said decryption means including said monitoring means.

23. The method of Claim 21 including the further steps of:

encrypting said first encryption key with a second encryption key; said second encryption key incorporated in said decryption means associated with said computer in which said software and data program is to be run; and

transmitting said first encryption key to said decryption means in an encrypted format.

24. The method of Claim 21 including the further step of erasing said software and data program from said computer when execution of said software and data program is complete, said operating system modification routine initiating said erasure of said software and data program.

25. The method of Claim 21 further including the step of destroying said first encryption key if said decryption means is tampered with in any manner.

26. The method of Claim 22 further including the step of periodically monitoring the state of said associated decryption means and monitoring means for determining if said associated decryption means and monitoring means is coupled to said computer, said operating system modification routine responsive to the occurrence of a periodic event associated with the execution of said software and data program to initiate said periodic monitoring of said associated decryption means and monitoring means.

27. The method of Claim 26 further including the step of erasing said software and data program from said computer and preventing the executing of said software and data program if said associated decryption means and monitoring means is decoupled from said computer.

28. A method of renting a software and data program for use on a customer's computer comprising the steps of:

storing said software and data program in said customer computer memory for use in said customer computer;

modifying the operating system of said customer computer utilizing an operating system modification routine;

modifying said use of said software and data program in said customer computer, said operating system modification routine responsive to a request to execute said software and data program to initiate said monitoring of said use for developing time accounting data; and

transmitting said time accounting data to a central host computer.

29. The method of Claim 28 further including the steps of :

storing said time accounting data; and

transmitting said time accounting data to said central host computer at preprogrammed times.

30. The method of Claim 29 further including the steps of:

monitoring the state of a time monitoring means associated with and coupled to said customer computer, said time monitoring means for monitoring said use of said software and data program in said customer computer; and

preventing said use of said software and data program if said time monitoring means is decoupled from said customer computer.

31. Apparatus as in Claim 4 further including activating means responsive to a first command from said first computer for activating said second computer.

32. Apparatus for renting computer programs for use in a user computer, said apparatus comprising:

a rental computer;

first transmitting and receiving means coupled to said rental computer for receiving information from said user computer; and

a second transmitting and receiving means coupled to said first transmitting and receiving means and to said user computer for transmitting information to said rental computer;

said first and second transmitting and receiving means each

including security means for preventing unauthorized use of said computer programs.

33. Apparatus as in Claim 32 wherein said security means includes encryption/decryption means for encrypting and decrypting, respectively, preselected portions of said computer program and a first encryption key for encrypting and decrypting said preselected portions of said computer program.

34. Apparatus as in Claim 33 wherein said first and second transmitting and receiving means each including a second encryption key for encrypting and decrypting, respectively, said first encryption key.

35. Apparatus as in Claim 33 wherein said encryption/ decryption means includes means for encrypting and decrypting different preselected portions of said computer programs.

36. Apparatus as in Claim 32 wherein;

said computer programs are stored in said rental computer;

said first transmitting and receiving means also transmits information including said computer programs to said user computer; and

said second transmitting and receiving means also receives information including said computer programs from said rental computer.

37. Apparatus as in Claim 36 wherein said security means includes encryption/decryption means for encrypting and decrypting, respectively, preselected portions of said computer program and a first encryption key for encrypting and decrypting said preselected portions of said computer program.

38. Apparatus as in Claim 37 wherein said first and second transmitting and receiving means each including a second encryption key for encrypting and decrypting, respectively, said first encryption key.

39. Apparatus as in Claim 37 wherein said encryption/ decryption means includes means for encrypting and decrypting different preselected portions of said computer programs.

40. Apparatus as in Claim 33 wherein said information includes

time accounting data for determining rental charges for use of said computer programs.

41. Apparatus as in Claim 36 further including monitoring means for monitoring usage by said user computer of the computer programs for developing time accounting data relative to rental charges for said usage, and for preventing usage of the computer programs if said second transmitting and receiving means is disconnected from said user computer.

42. Apparatus as in Claim 41 further including memory means coupled to said monitoring means for storing said time accounting data, said second transmitting and receiving means being responsive to a first from said rental computer for transmitting said time accounting data to said rental computer.

43. Apparatus as in Claim 42 further including:

error detection means for detecting the presence of an error in said time accounting data transmitted by said second transmitting and receiving means and for producing an error signal; and

retransmission means coupled to said error detection means and responsive to said error signal for producing a signal representing a request for retransmission of said time accounting data, said second transmitting and receiving means responsive to said request for retransmission for retransmitting said time accounting data.

44. Apparatus as in Claim 43 further including activating means responsive to a first command from said second computer for activating said second computer.

45. A software rental system for renting computer game software for use in a user game computer, said software rental system comprising:

a central computer for storing a plurality of selectable game software packages;

first transmitting and receiving means coupled to said central

computer for transmitting information and selected ones of said plurality of selectable game software packages to a user game computer and for receiving information from said user game computer;

second transmitting and receiving means coupled to said first transmitting and receiving means and to said user game computer for transmitting information to said central computer and for receiving information and selected ones of said plurality of selectable game software packages from said central computer; and

said first and second transmitting and receiving means each including security means for preventing unauthorized use of said selected game software packages.

46. A software rental system as in Claim 45 further comprising interface means coupled between said user game computer and said second transmitting and receiving means, said interface means for adapting said second transmitting and receiving means to said user game computer.

47. A software rental system as in Claim 46 wherein said interface means comprises a plug-in cartridge adapted for use with a plug-in slot provided in said user game computer.

48. A software rental system as in Claim 46 wherein said security means includes encryption/decryption means for encrypting and decrypting, respectively, said game software and a first encryption key for encrypting and decrypting said game software.

49. A software rental system as in Claim 48 wherein said second transmitting and receiving means includes a second encryption key for encrypting and decrypting, respectively, said first encryption key.

50. A software rental system as in Claim 49 wherein selected portions of said game software are encrypted prior to transmission by said first transmitting and receiving means.

51. A software rental system as in Claim 48 wherein said first encryption key comprises a unique software package identifier code.

52. A software rental system as in Claim 49 wherein said first

encryption key comprises a unique software package identifier code, a different software package identifier code being associated with each of said plurality of selectable game software packages.

53. A software rental system as in Claim 52 wherein said second encryption key comprises a unique user identifier code, each user being assigned a different unique user identifier code.

54. A software rental system as in Claim 46 wherein said second transmitting and receiving means includes storage means for storing said selected game software packages and information transmitted from said central computer.

55. A software rental system as in claim 54 wherein said stored information includes menus providing information related to said plurality of selectable game software packages.

56. A software rental system as in Claim 54 further comprising user input means coupled to said user game computer for selecting desired ones of said plurality of selectable game software packages for transmission to said user game computer.

57. A software rental system as in Claim 56 further comprising display means coupled to said user game computer for displaying a menu providing descriptive information related to said plurality of selectable game software packages, said descriptive information including game software package selection data.

58. A software rental system as in Claim 45 wherein said information includes time accounting data for determining rental charges for use of said game software packages.

59. A software rental system as in Claim 56 further including monitoring means for monitoring usage by said user game computer of said selected game software packages for developing time accounting data relative to rental charges for said usage, and for preventing usage of said game software packages if said second transmitting and receiving means is disconnected from said user game computer.

60. A software rental system as in Claim 59 further including memory means coupled to said monitoring means for storing said time accounting data, said second transmitting and receiving means being responsive to a command from said central computer for transmitting said time accounting data to said central computer.

61. A software rental system as in Claim 60 further including:

error detection means for detecting the presence of an error in said time accounting data transmitted by said second transmitting and receiving means and for producing an error signal; and

retransmission means coupled to said error detection means and responsive to said error signal for producing a signal representing a request for retransmission of said time accounting data, said second transmitting and receiving means responsive to said request for retransmission for retransmitting said time accounting data.

62. A method of renting computer game software for use in a user game computer comprising the steps of:

storing a plurality of selectable game software packages in a central computer;

encrypting said plurality of selectable game software packages;

transmitting selected ones of said plurality of selectable game software packages to a user;

receiving and decrypting said transmitted game software packages;

monitoring use of said transmitted game software packages in a user game computer for developing time accounting data; and

transmitting said time accounting data to said central computer.

63. The method as in Claim 62 further including the step of storing said transmitted game software packages for repeated use in said user game computer.

64. The method as in Claim 62 wherein said step of encrypting said plurality of selectable game software packages comprises encrypting selected

critical portions of each of said plurality of selectable game software packages.

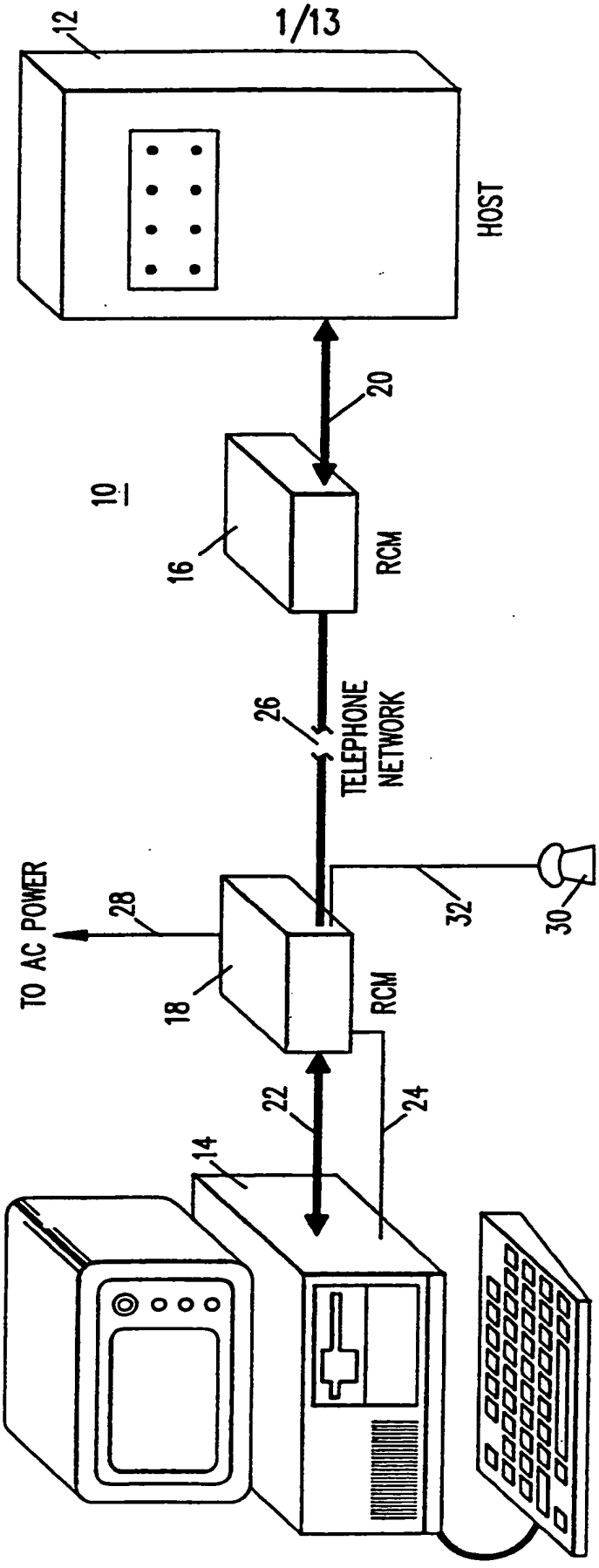

12
HOST
20
10
16
RCM
26
TELEPHONE NETWORK
TO AC POWER
28
18
RCM
32
30
22
24
14
TARGET

FIG. 1

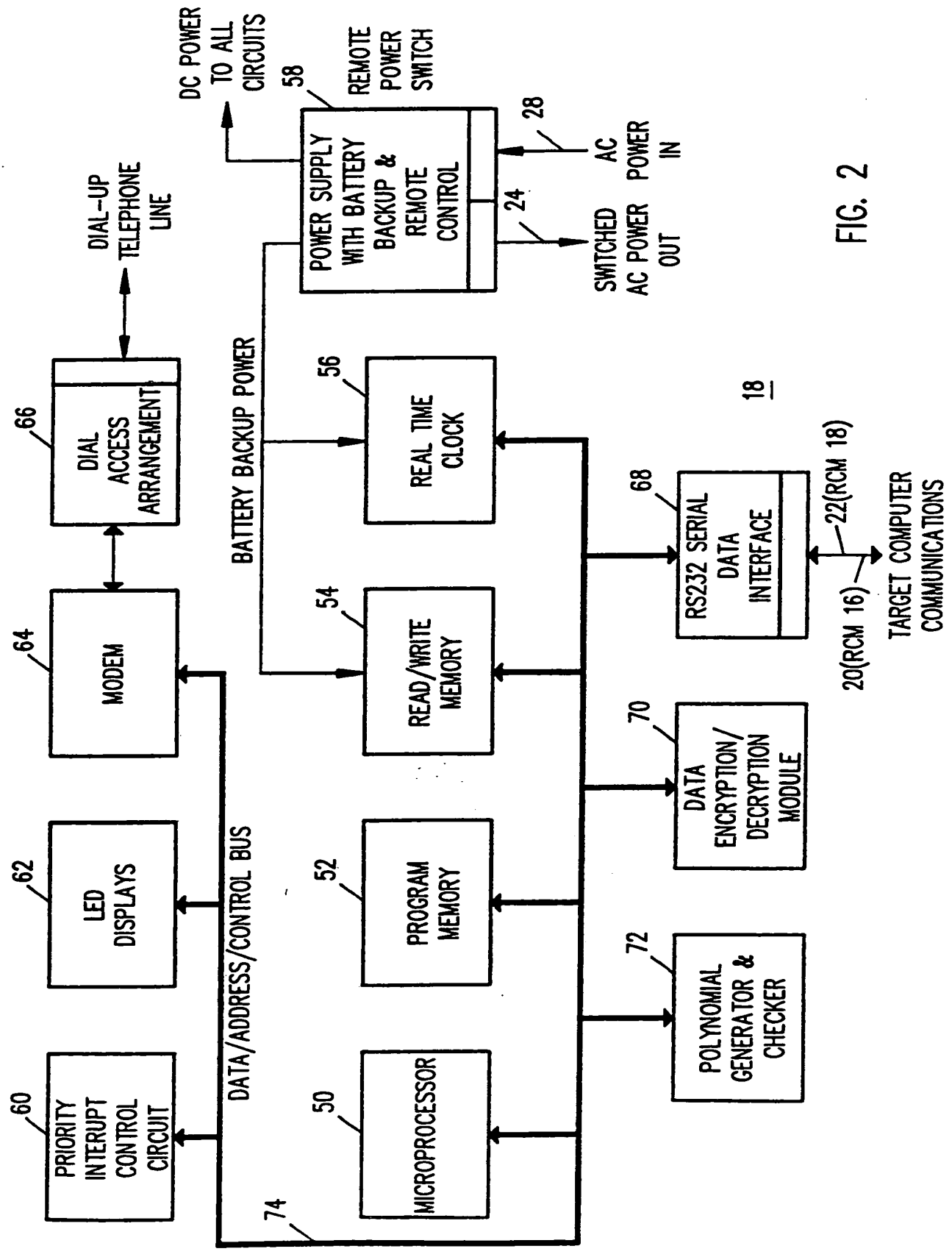

DC POWER TO ALL CIRCUITS
58
REMOTE POWER SWITCH
28
AC POWER IN
24
SWITCHED AC POWER OUT
POWER SUPPLY WITH BATTERY BACKUP & REMOTE CONTROL
DIAL-UP TELEPHONE LINE
66
DIAL ACCESS ARRANGEMENT
BATTERY BACKUP POWER
56
REAL TIME CLOCK
18
68
RS232 SERIAL DATA INTERFACE
22(RCM 18)
20(RCM 16)
TARGET COMPUTER COMMUNICATIONS
64
MODEM
54
READ/WRITE MEMORY
70
DATA ENCRYPTION/ DECRYPTION MODULE
62
LED DISPLAYS
52
PROGRAM MEMORY
72
POLYNOMIAL GENERATOR & CHECKER
60
PRIORITY INTERUPT CONTROL CIRCUIT
DATA/ADDRESS/CONTROL BUS
50
MICROPROCESSOR
74

FIG. 2

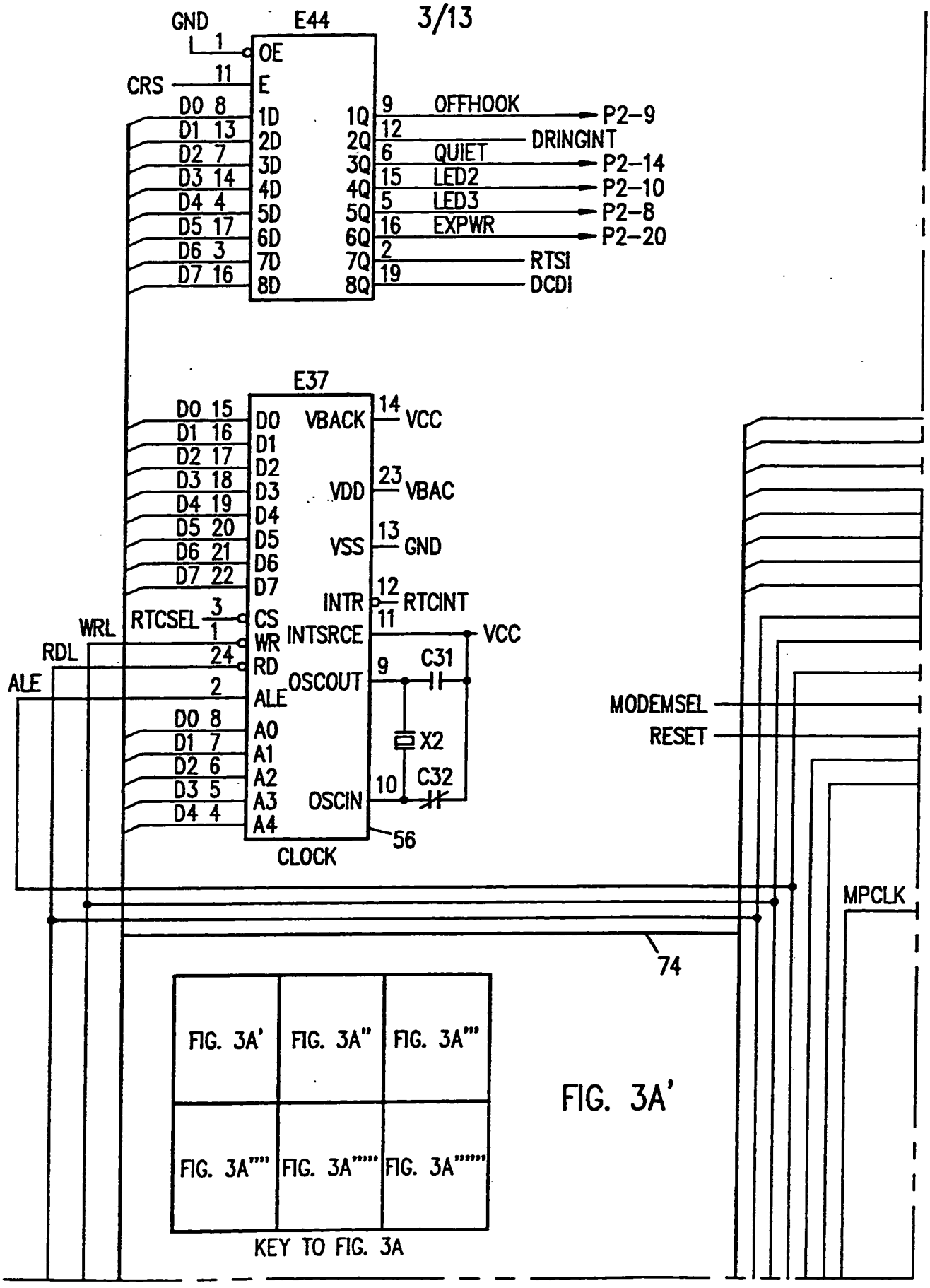

GND
E44
1 OE
CRS 11 E
D0 8 1D
D1 13 2D
D2 7 3D
D3 14 4D
D4 4 5D
D5 17 6D
D6 3 7D
D7 16 8D
1Q 9 OFFHOOK P2-9
2Q 12 DRINGINT
3Q 6 QUIET P2-14
4Q 15 LED2 P2-10
5Q 5 LED3 P2-8
6Q 16 EXPWR P2-20
7Q 2 RTSI
8Q 19 DCDI
E37
D0 15 D0
D1 16 D1
D2 17 D2
D3 18 D3
D4 19 D4
D5 20 D5
D6 21 D6
D7 22 D7
VBACK 14 VCC
VDD 23 VBAC
VSS 13 GND
INTR 12 RTCINT
RTCSEL 3 CS
WRL 1 WR
RDL 24 RD
ALE 2 ALE
INTSRCE 11 VCC
OSCOUT 9 C31
X2
OSCIN 10 C32
D0 8 A0
D1 7 A1
D2 6 A2
D3 5 A3
D4 4 A4
56
CLOCK
MODEMSEL
RESET
MPCLK
74

FIG. 3A'
FIG. 3A"
FIG. 3A'''
FIG. 3A''''
FIG. 3A'''''
FIG. 3A''''''
KEY TO FIG. 3A

FIG. 3A'

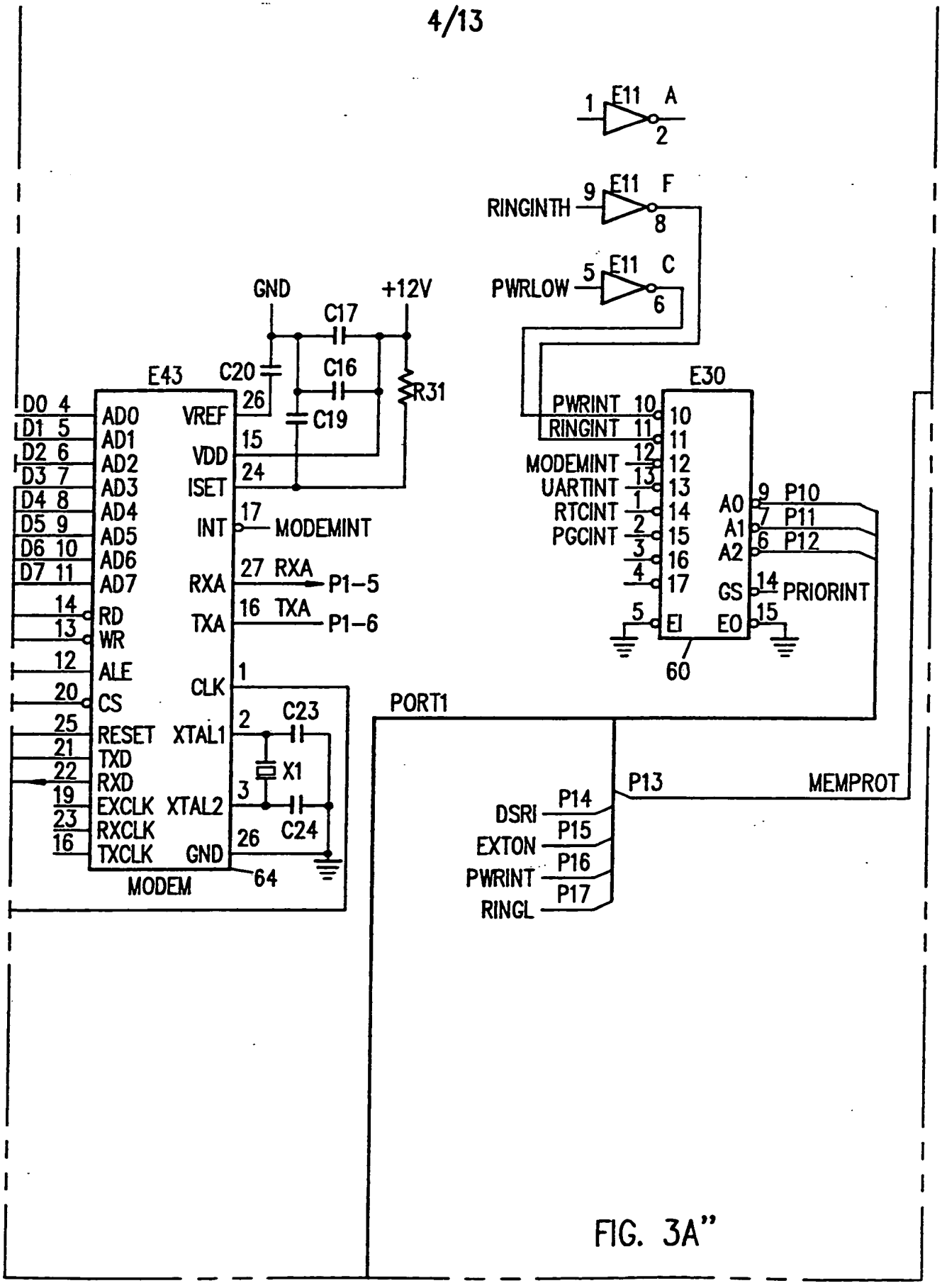

E11 A
E11 F
E11 C
RINGINTH
PWRLOW
GND
+12V
C17
C20
C16
C19
R31
E43
E30
D0 4
D1 5
D2 6
D3 7
D4 8
D5 9
D6 10
D7 11
AD0
AD1
AD2
AD3
AD4
AD5
AD6
AD7
VREF
VDD
ISET
INT
RXA
TXA
MODEMINT
P1-5
P1-6
RD
WR
ALE
CS
RESET
TXD
RXD
EXCLK
RXCLK
TXCLK
CLK
XTAL1
XTAL2
GND
C23
X1
C24
MODEM
64
PWRINT
RINGINT
MODEMINT
UARTINT
RTCINT
PGCINT
A0
A1
A2
GS
EI
EO
P10
P11
P12
PRIORINT
60
PORT1
P13
MEMPROT
DSRI
EXTON
PWRINT
RINGL
P14
P15
P16
P17

FIG. 3A"

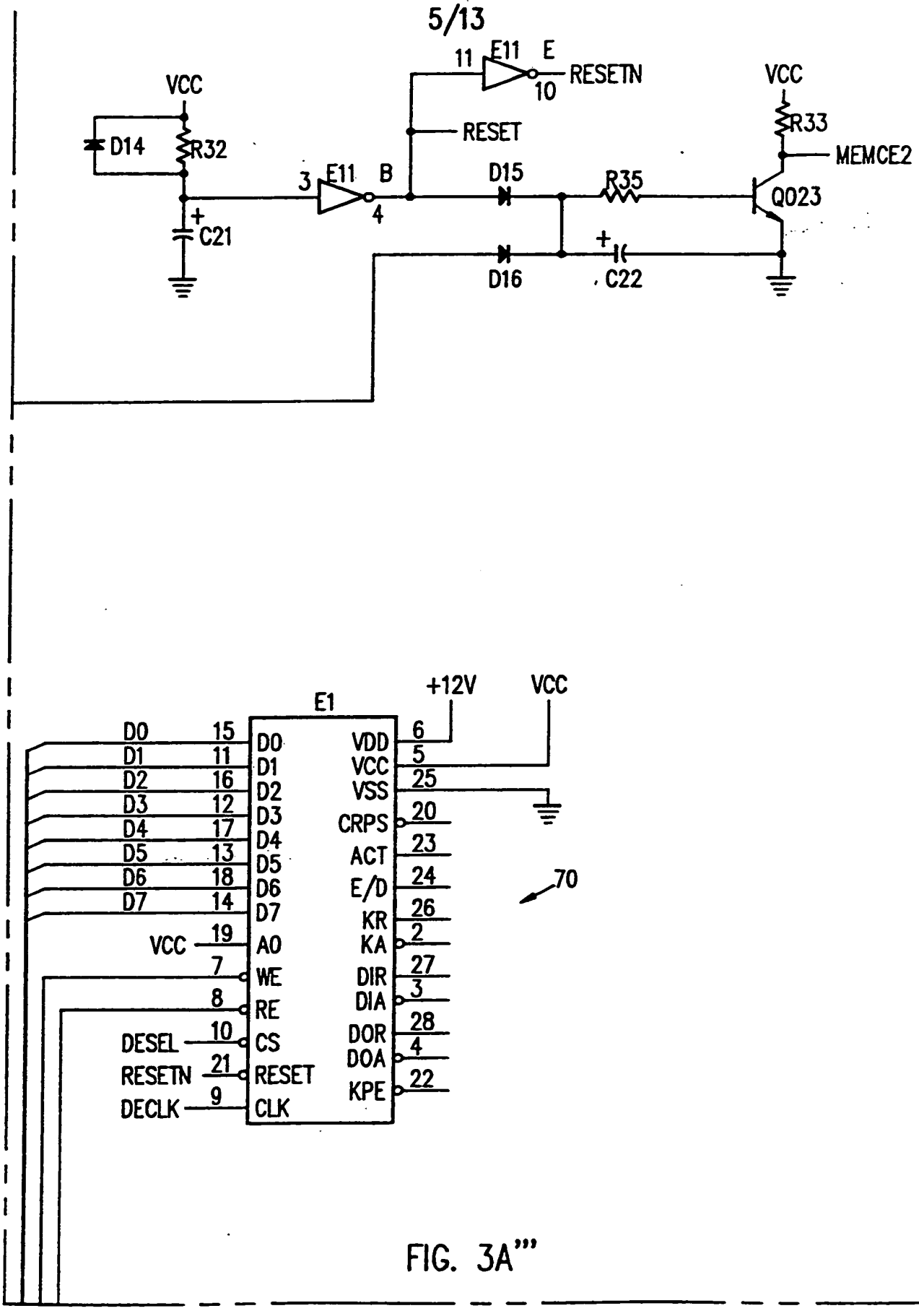

VCC
D14
R32
C21
3
E11
B
4
11
E11
E
10
RESETN
RESET
D15
D16
R35
C22
VCC
R33
MEMCE2
Q023
E1
+12V
VCC
D0
D1
D2
D3
D4
D5
D6
D7
VCC
DESEL
RESETN
DECLK
15
11
16
12
17
13
18
14
19
7
8
10
21
9
D0
D1
D2
D3
D4
D5
D6
D7
A0
WE
RE
CS
RESET
CLK
VDD
VCC
VSS
CRPS
ACT
E/D
KR
KA
DIR
DIA
DOR
DOA
KPE
6
5
25
20
23
24
26
2
27
3
28
4
22
70

FIG. 3A'''

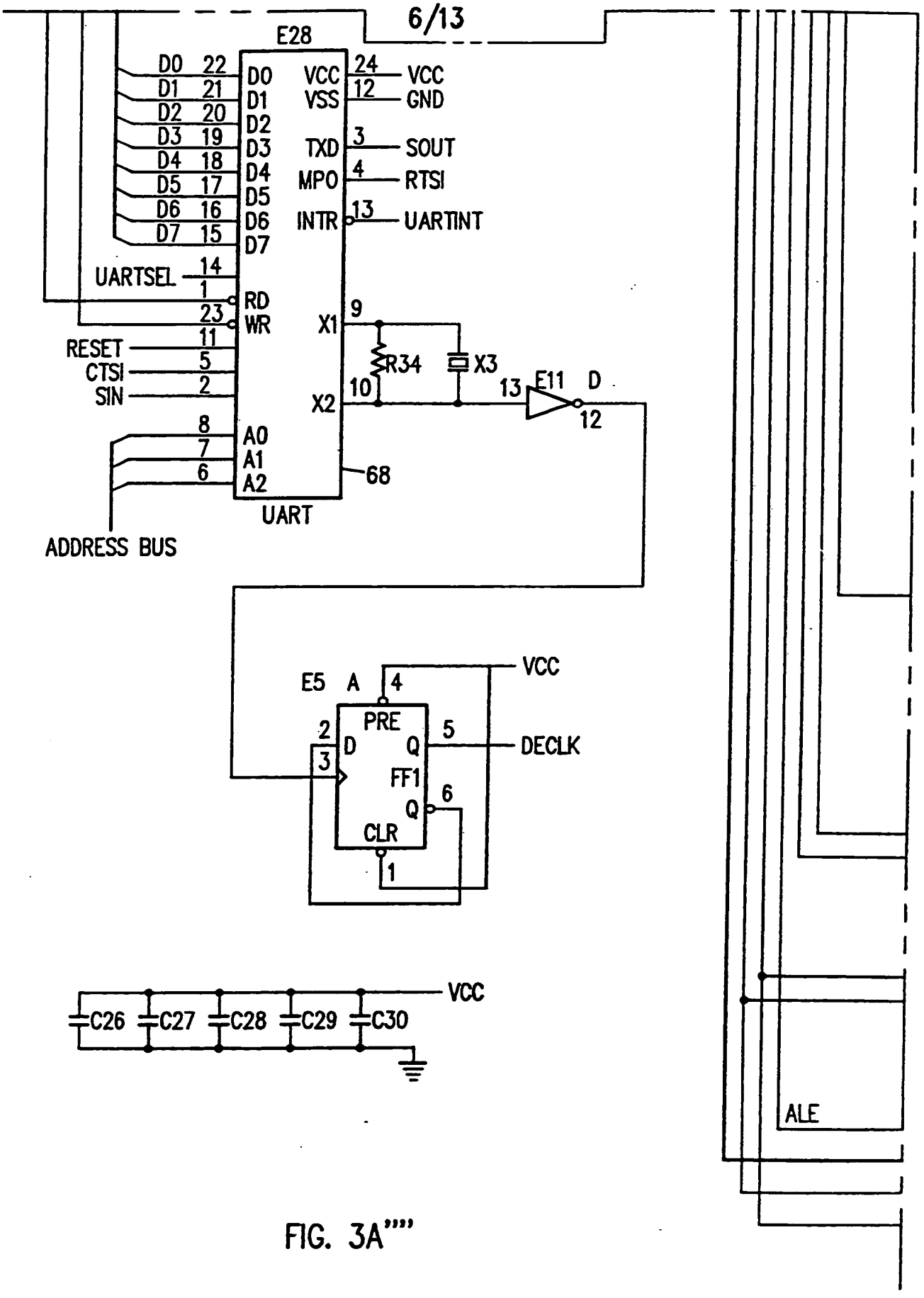

E28
D0 22
D1 21
D2 20
D3 19
D4 18
D5 17
D6 16
D7 15
UARTSEL 14
1
23
RESET 11
CTSI 5
SIN 2
8
7
6
D0
D1
D2
D3
D4
D5
D6
D7
RD
WR
A0
A1
A2
VCC 24
VSS 12
TXD 3
MPO 4
INTR 13
X1 9
X2 10
68
VCC
GND
SOUT
RTSI
UARTINT
R34
X3
E11 D
13
12
UART
ADDRESS BUS
E5 A 4
PRE
2
D
3
FF1
CLR
1
Q 5
Q 6
DECLK
VCC
C26
C27
C28
C29
C30
VCC
ALE

FIG. 3A''''

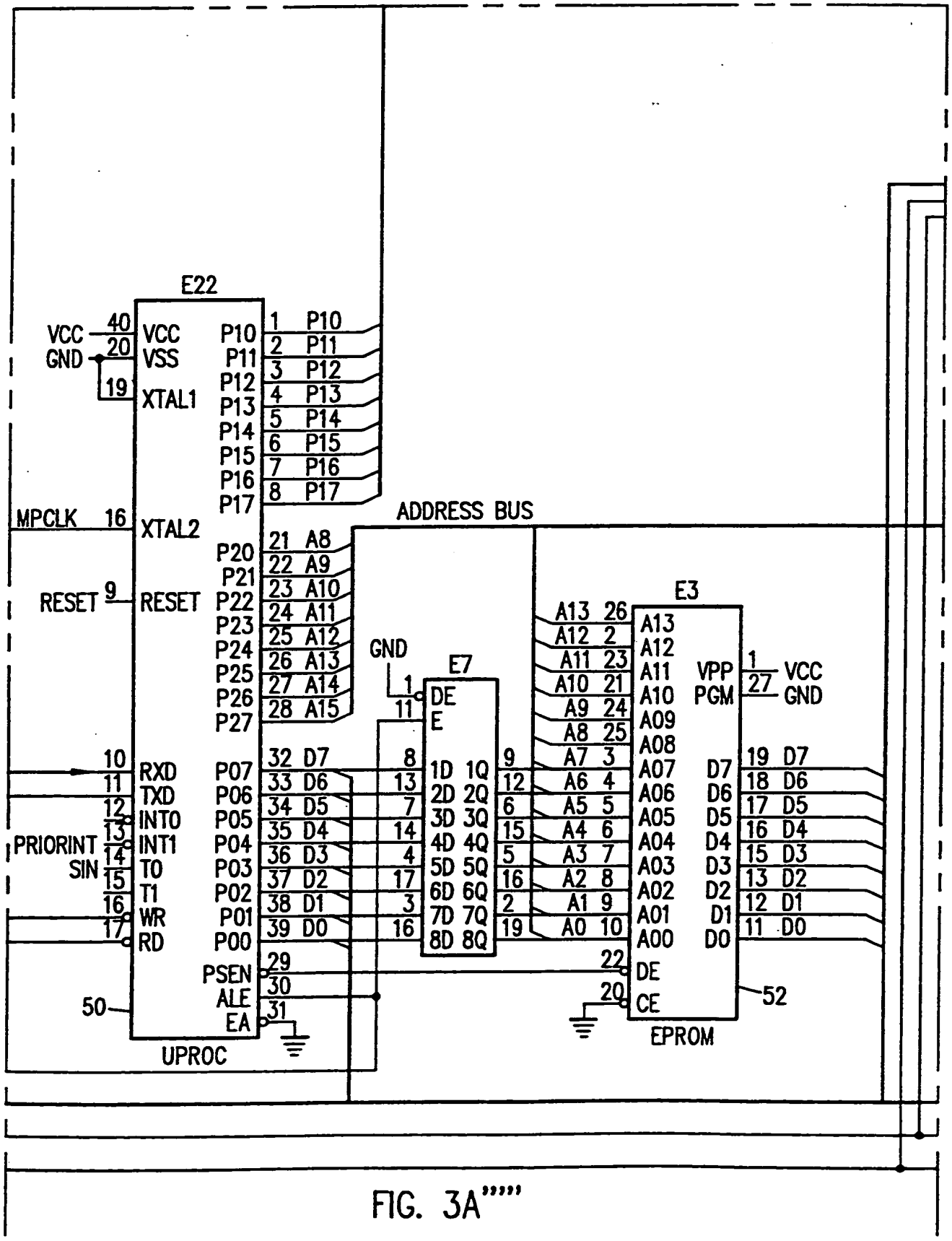

E22
VCC 40 VCC
GND 20 VSS
19 XTAL1
MPCLK 16 XTAL2
RESET 9 RESET
10 RXD
11 TXD
12 INT0
13 INT1
PRIORINT
14 T0
SIN
15 T1
16 WR
17 RD
50
P10 1 P10
P11 2 P11
P12 3 P12
P13 4 P13
P14 5 P14
P15 6 P15
P16 7 P16
P17 8 P17
P20 21 A8
P21 22 A9
P22 23 A10
P23 24 A11
P24 25 A12
P25 26 A13
P26 27 A14
P27 28 A15
P07 32 D7
P06 33 D6
P05 34 D5
P04 35 D4
P03 36 D3
P02 37 D2
P01 38 D1
P00 39 D0
PSEN 29
ALE 30
EA 31
UPROC
ADDRESS BUS
GND
E7
1 DE
11 E
8 1D 1Q 9
13 2D 2Q 12
7 3D 3Q 6
14 4D 4Q 15
4 5D 5Q 5
17 6D 6Q 16
3 7D 7Q 2
16 8D 8Q 19
E3
A13 26 A13
A12 2 A12
A11 23 A11
A10 21 A10
A9 24 A09
A8 25 A08
A7 3 A07
A6 4 A06
A5 5 A05
A4 6 A04
A3 7 A03
A2 8 A02
A1 9 A01
A0 10 A00
22 DE
20 CE
VPP 1 VCC
PGM 27 GND
D7 19 D7
D6 18 D6
D5 17 D5
D4 16 D4
D3 15 D3
D2 13 D2
D1 12 D1
D0 11 D0
52
EPROM

FIG. 3A''''

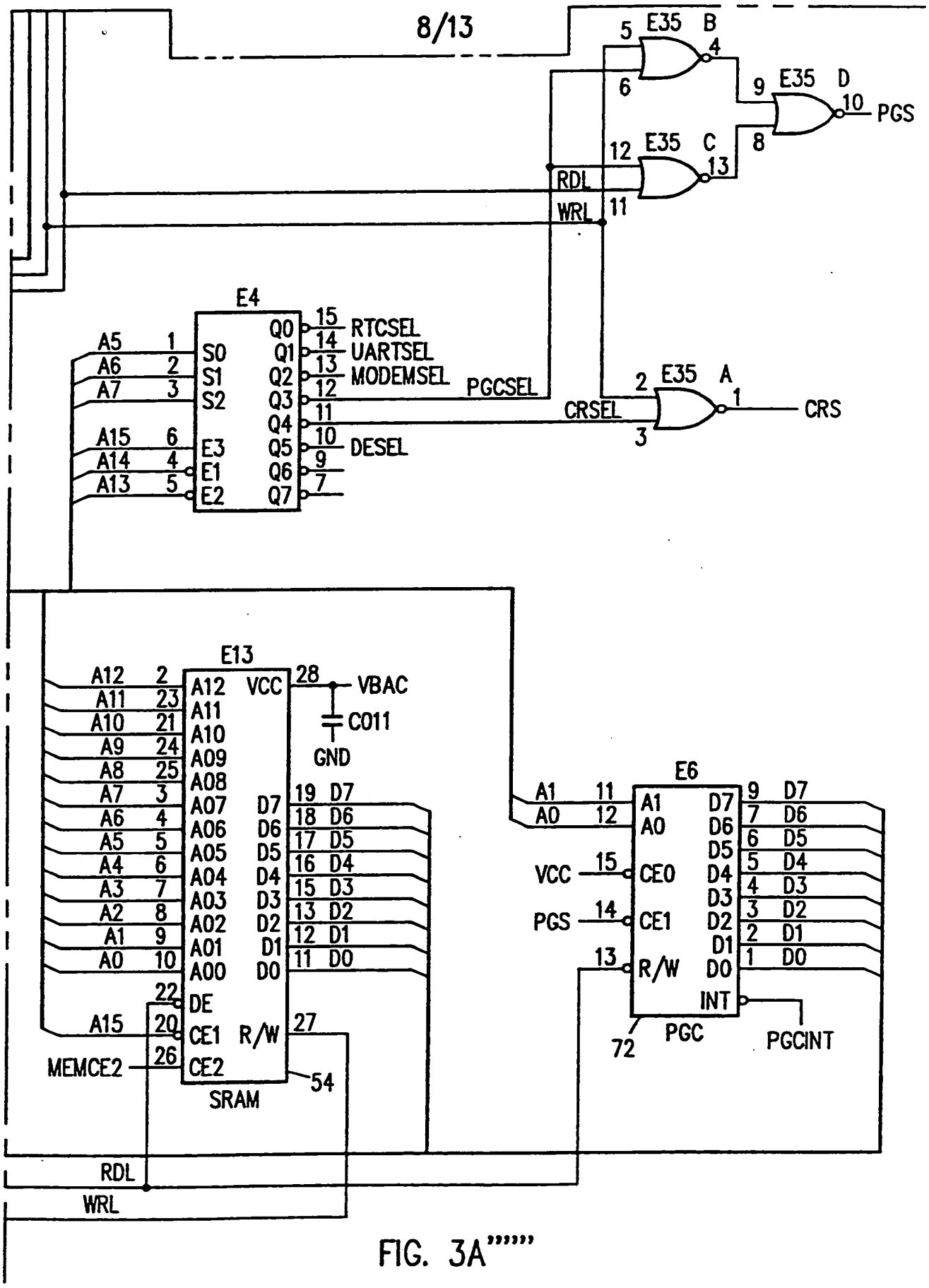

8/13
E35 B
E35 D
PGS
E35 C
RDL
WRL
E4
RTCSEL
UARTSEL
MODEMSEL
PGCSEL
DESEL
E35 A
CRSEL
CRS
E13
VBAC
C011
GND
SRAM
MEMCE2
E6
VCC
PGS
R/W
INT
PGC
72
PGCINT
RDL
WRL

FIG. 3A''''''

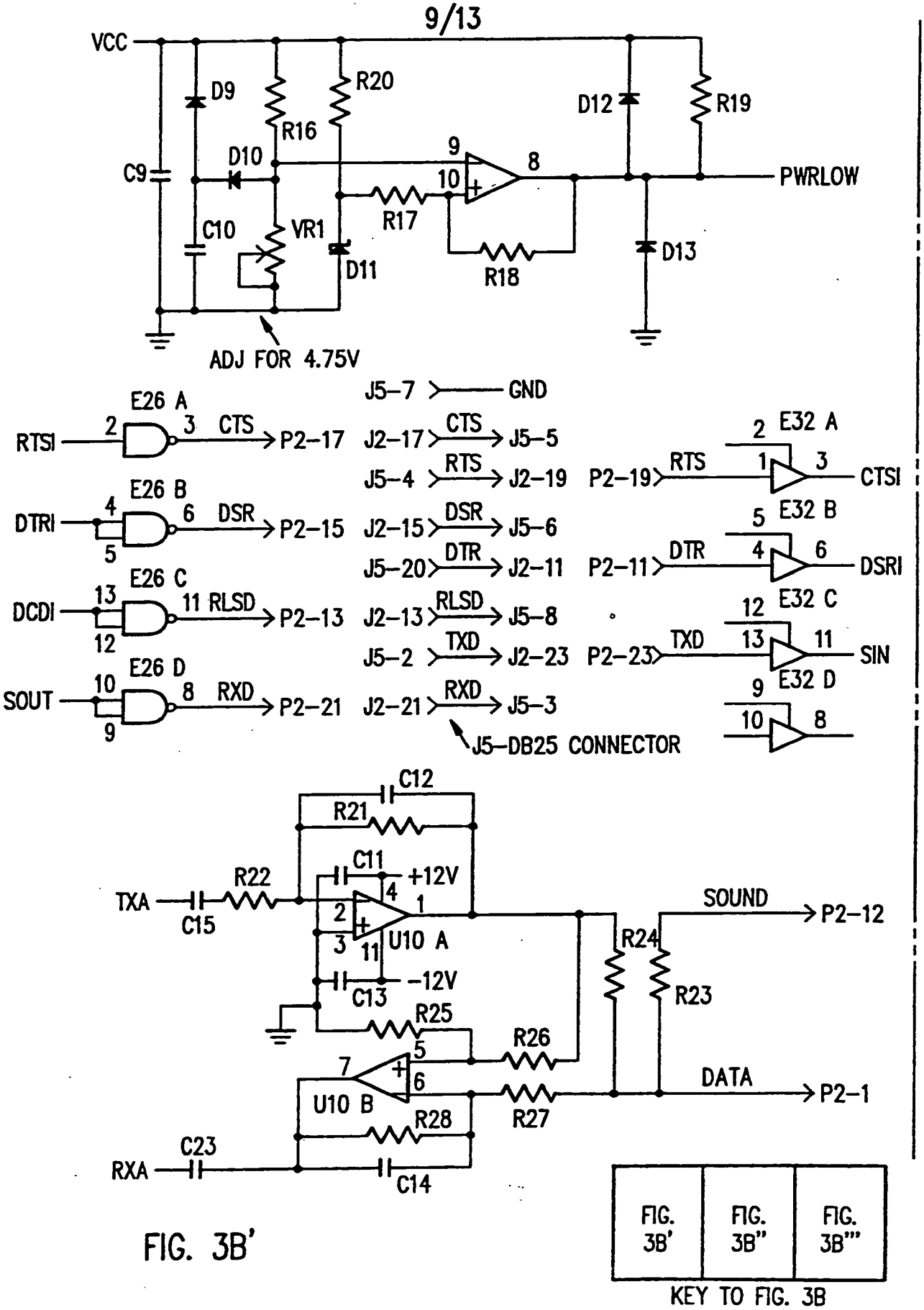


FIG. 3B'

FIG. 3B'	FIG. 3B"	FIG. 3B"'

KEY TO FIG. 3B

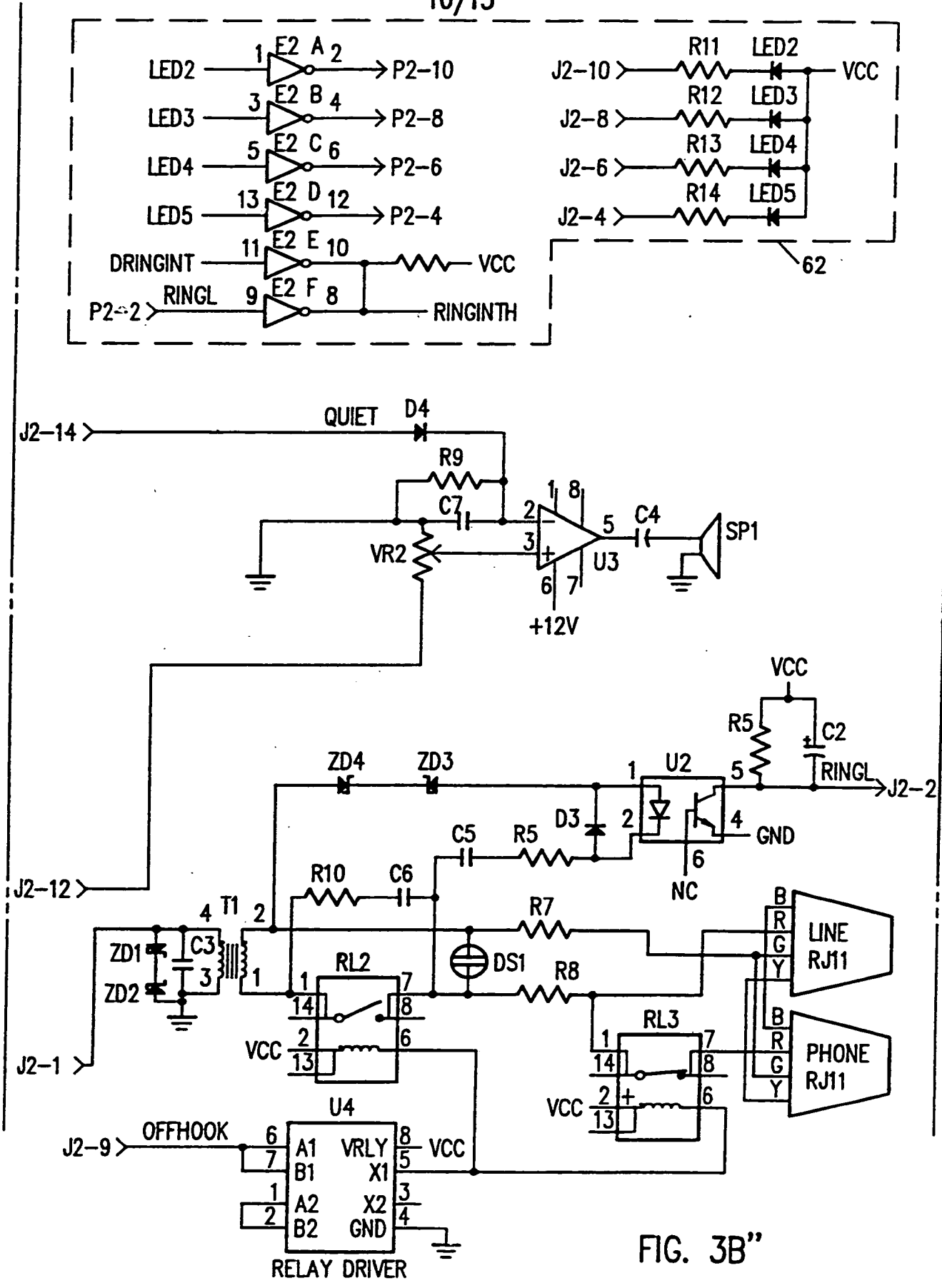

LED2
LED3
LED4
LED5
DRINGINT
RINGL
P2-2
P2-10
P2-8
P2-6
P2-4
VCC
RINGINTH
J2-10
J2-8
J2-6
J2-4
R11
R12
R13
R14
62
J2-14
QUIET
D4
R9
C7
VR2
U3
C4
SP1
+12V
J2-12
J2-1
ZD4
ZD3
U2
R5
C2
RINGL
J2-2
GND
NC
D3
C5
R10
C6
T1
ZD1
ZD2
C3
RL2
DS1
R7
R8
LINE RJ11
RL3
PHONE RJ11
U4
J2-9
OFFHOOK
A1
B1
A2
B2
VRLY
X1
X2
GND
RELAY DRIVER

FIG. 3B"

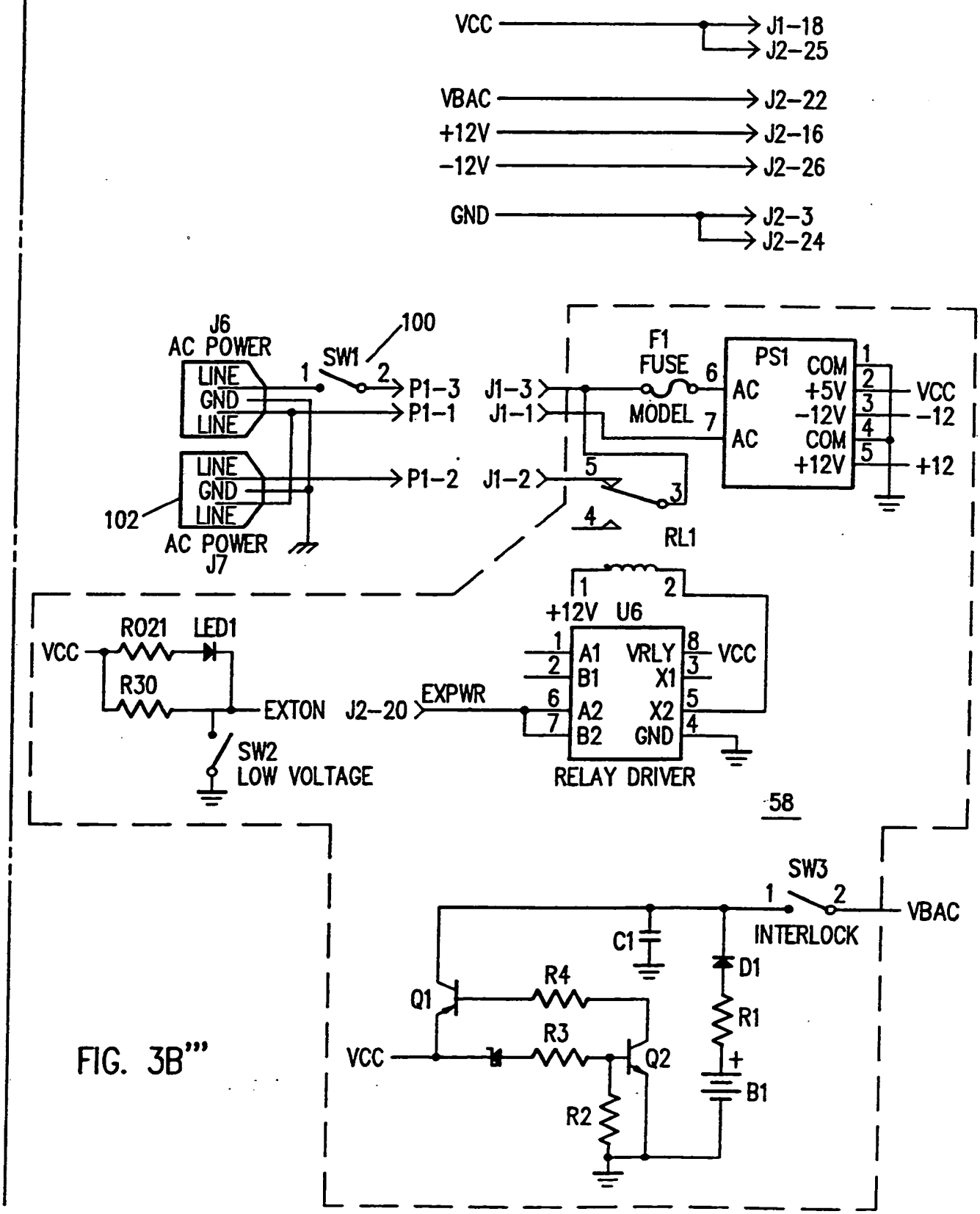

VCC
J1-18
J2-25
VBAC
J2-22
+12V
J2-16
-12V
J2-26
GND
J2-3
J2-24
J6
AC POWER
LINE
GND
LINE
SW1
100
P1-3
P1-1
P1-2
102
AC POWER
J7
J1-3
J1-1
J1-2
F1
FUSE
MODEL
PS1
AC
AC
COM
+5V
-12V
COM
+12V
VCC
-12
+12
RL1
+12V U6
A1
B1
A2
B2
VRLY
X1
X2
GND
RELAY DRIVER
R021
LED1
R30
EXTON
J2-20
EXPWR
SW2
LOW VOLTAGE
58
SW3
INTERLOCK
VBAC
C1
D1
R1
B1
Q1
R4
R3
Q2
R2
VCC

FIG. 3B'''

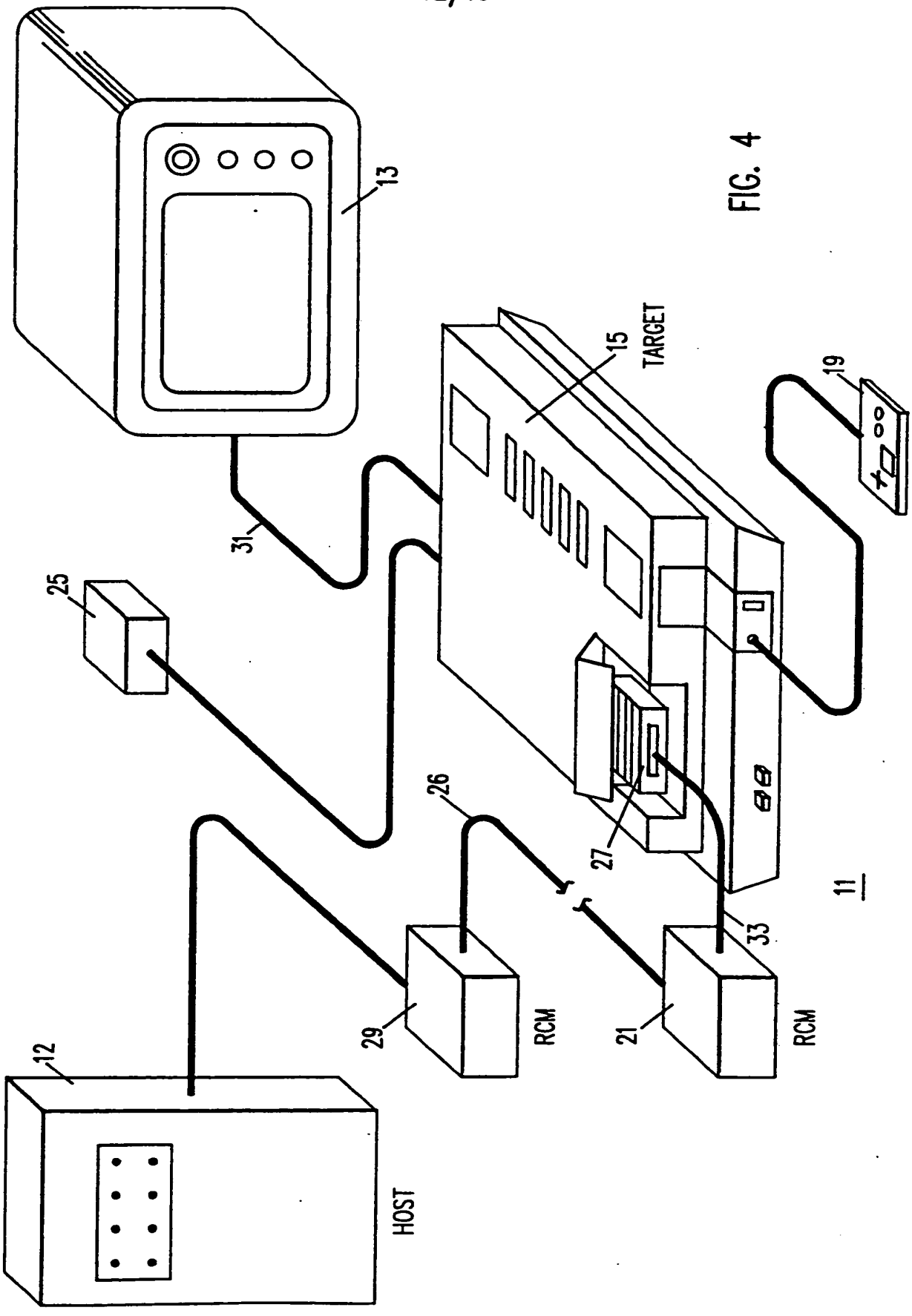


FIG. 4

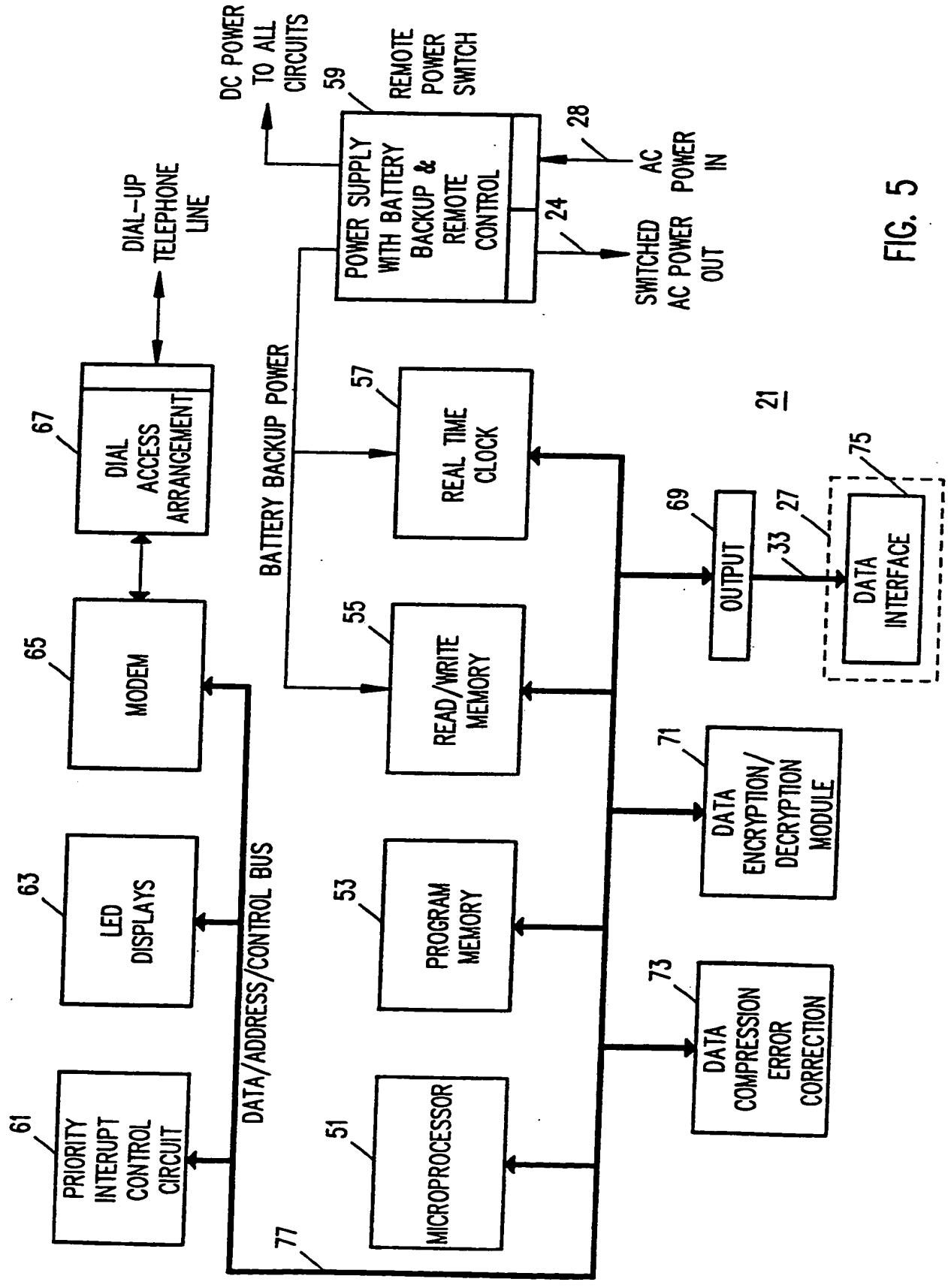

DC POWER TO ALL CIRCUITS
59
REMOTE POWER SWITCH
28
AC POWER IN
24
SWITCHED AC POWER OUT
POWER SUPPLY WITH BATTERY BACKUP & REMOTE CONTROL
DIAL-UP TELEPHONE LINE
67
DIAL ACCESS ARRANGEMENT
BATTERY BACKUP POWER
57
REAL TIME CLOCK
21
75
69
27
33
OUTPUT
DATA INTERFACE
65
MODEM
55
READ/WRITE MEMORY
71
DATA ENCRYPTION/ DECRYPTION MODULE
63
LED DISPLAYS
53
PROGRAM MEMORY
73
DATA COMPRESSION ERROR CORRECTION
61
PRIORITY INTERUPT CONTROL CIRCUIT
DATA/ADDRESS/CONTROL BUS
51
MICROPROCESSOR
77

FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 90/02209

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) *

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[5]: G 06 F 1/00, G 06 F 12/14

II. FIELDS SEARCHED

Minimum Documentation Searched 7

Classification System	Classification Symbols
IPC[5]	G 06 F

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched 8

III. DOCUMENTS CONSIDERED TO BE RELEVANT 9

Category *	Citation of Document, 11 with indication, where appropriate, of the relevant passages 12	Relevant to Claim No. 13
X	WO, A, 88/02960 (PERSONAL LIBRARY SOFTWARE) 21 April 1988 see page 20, line 4 - page 21, line 3; page 24, line 22 - page 25, line 17; page 26, lines 11-27; page 29, line 14 - page 33, line 4; page 36, line 20 - page 39, line 32; page 42, line 14 - page 44, line 5; figures 1,3	1-3,5,7,10
A		4,6,8,11,12, 16,17,20,28, 32,45,62
	--	
X	WO, A, 85/02310 (SOFTNET INC.) 23 May 1985 see page 8, line 3 - page 15, line 2; figures 1,2	45,46,48,50, 51
A		1,10,11,20, 28,32,45,49, 62
	--	
	./.	

* Special categories of cited documents: 10

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
28th August 1990	28. 09. 90
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	H. Ballesteros

Form PCT/ISA/210 (second sheet) (January 1985)

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category *	Citation of Document, ** with indication, where appropriate, of the relevant passages	Relevant to Claim No.
A	WO, A, 88/02202 (M/A-COM GOVERNMENT SYSTEMS) 24 March 1988 see page 3, line 1 - page 7, line 8; figures 1,2 --	1,10,20,28, 32
A	WO, A, 85/03584 (GUIGNARD) 15 August 1985 see page 4, line 15 - page 8, line 3; page 13, line 15 - page 15, line 33 ----------	1,10,20,28, 32

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. US 9002209 SA 36860

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 21/09/90
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A- 8802960	21-04-88	EP-A-	0329681	30-08-89
WO-A- 8502310	23-05-85	EP-A-	0161310	21-11-85
		GB-A-	2149944	19-06-85
WO-A- 8802202	24-03-88	AU-A-	8024787	07-04-88
		EP-A-	0282570	21-09-88
		JP-T-	1501274	27-04-89
WO-A- 8503584	15-08-85	AU-A-	3930185	27-08-85
		EP-A-	0203066	03-12-86